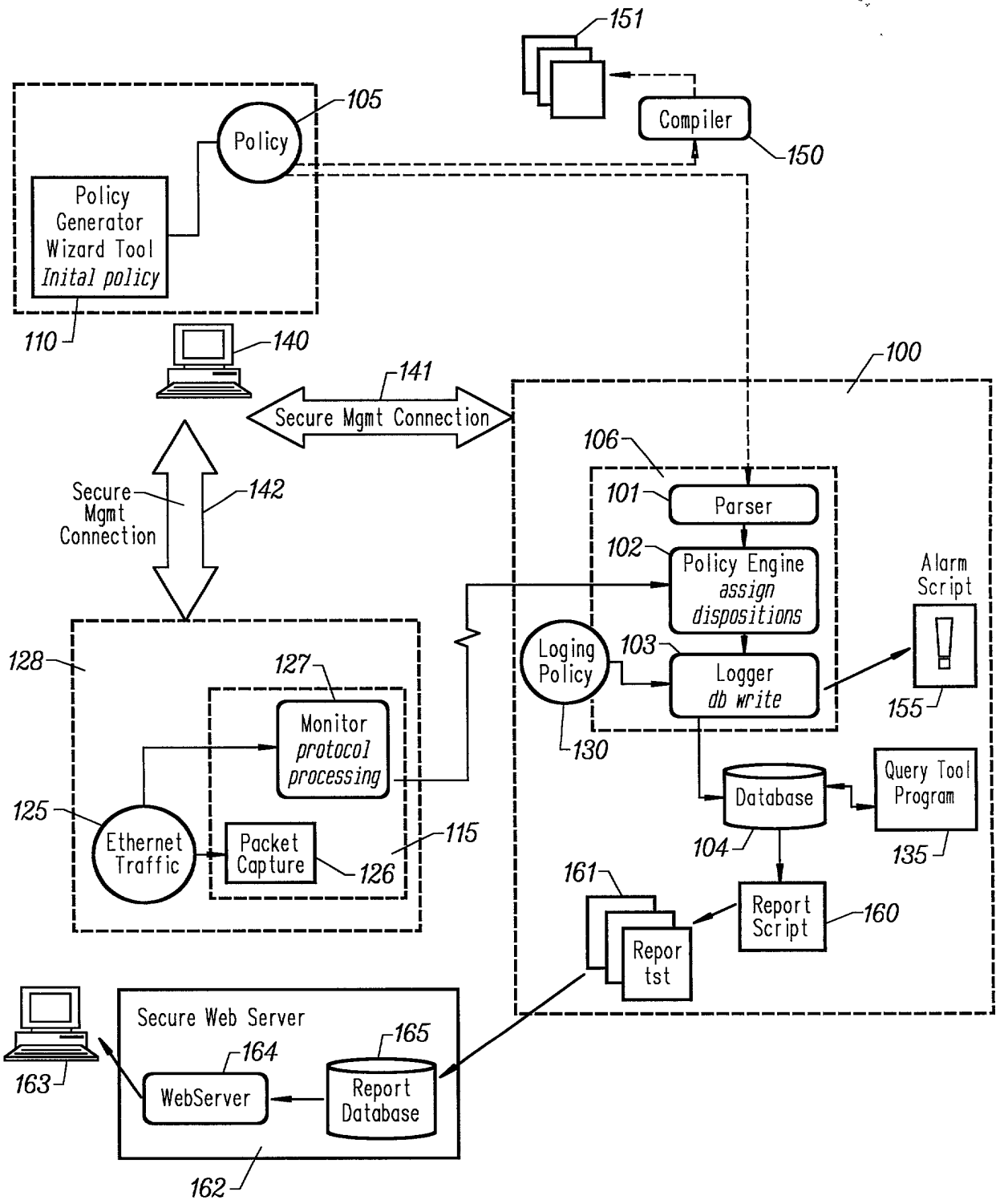

151
Compiler
150
105
Policy
Policy Generator Wizard Tool
Inital policy
110
140
141
Secure Mgmt Connection
100
106
101
Parser
102
Policy Engine
assign dispositions
Alarm Script
103
Loging Policy
Logger
db write
155
130
Secure Mgmt Connection
142
128
127
Monitor
protocol processing
125
Ethernet Traffic
Packet Capture
126
115
Database
Query Tool Program
104
135
161
Report Script
160
Repor tst
Secure Web Server
165
164
163
WebServer
Report Database
162

FIG. 1A

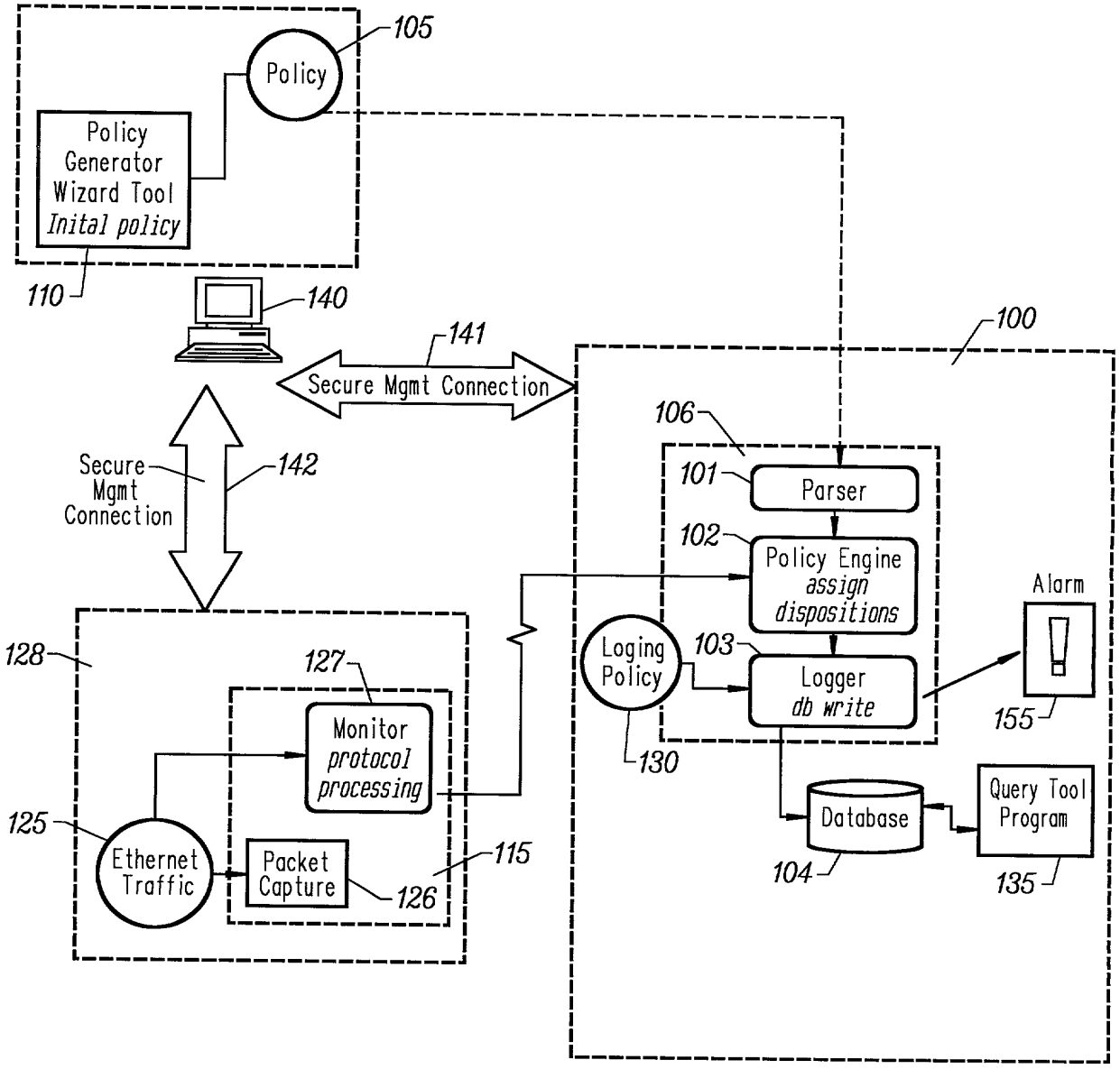

105
Policy
Policy Generator Wizard Tool
Inital policy
110
140
141
Secure Mgmt Connection
100
106
Secure Mgmt Connection
142
101
Parser
102
Policy Engine
assign dispositions
Alarm
Loging Policy
103
Logger
db write
155
130
128
127
Monitor
protocol processing
125
Ethernet Traffic
Packet Capture
126
115
Database
Query Tool Program
104
135

FIG. 1B

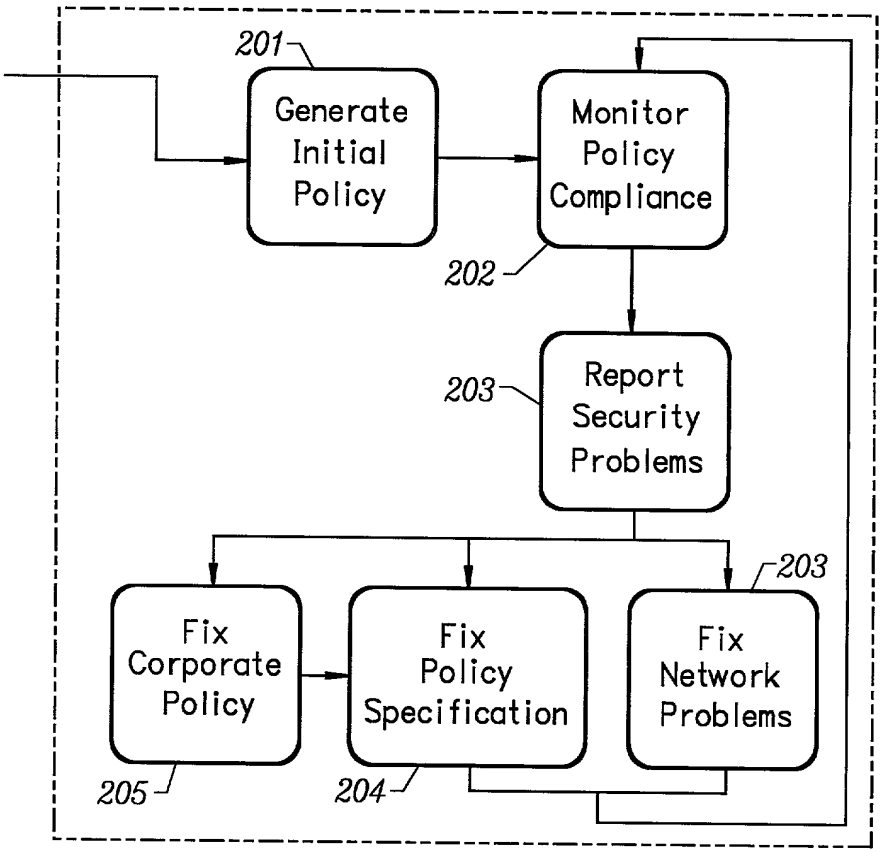

201
Generate Initial Policy
Monitor Policy Compliance
202
203
Report Security Problems
203
Fix Corporate Policy
Fix Policy Specification
Fix Network Problems
205
204

FIG. 2

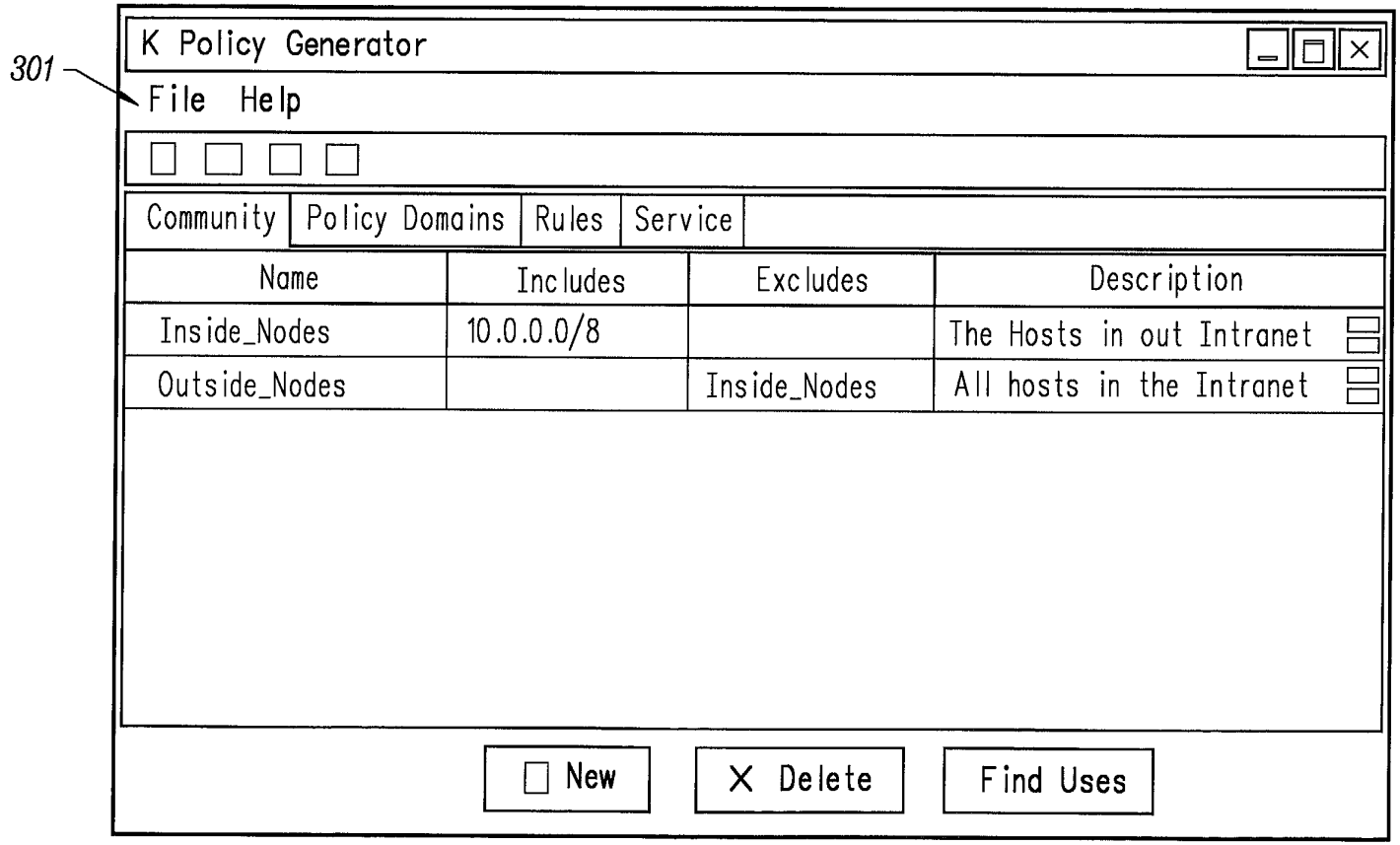

301
K Policy Generator
File Help
Community
Policy Domains
Rules
Service
Name
Includes
Excludes
Description
Inside_Nodes
10.0.0.0/8
The Hosts in out Intranet
Outside_Nodes
Inside_Nodes
All hosts in the Intranet
New
Delete
Find Uses

FIG. 3

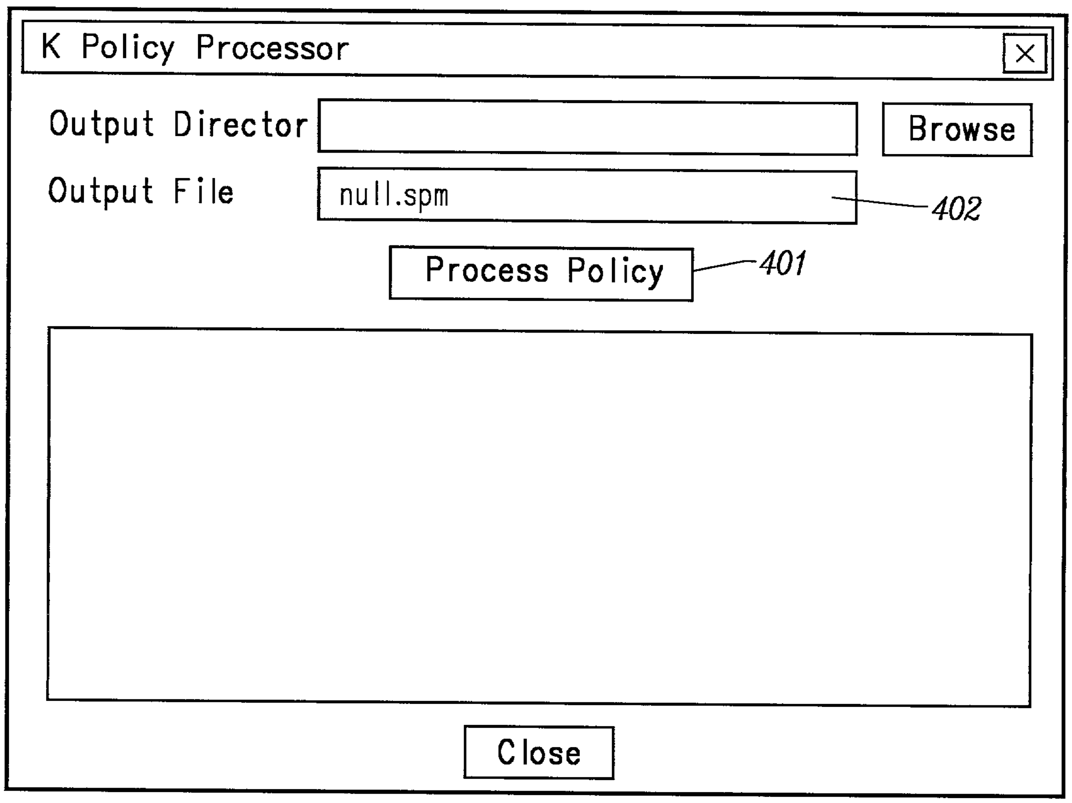


FIG. 4A

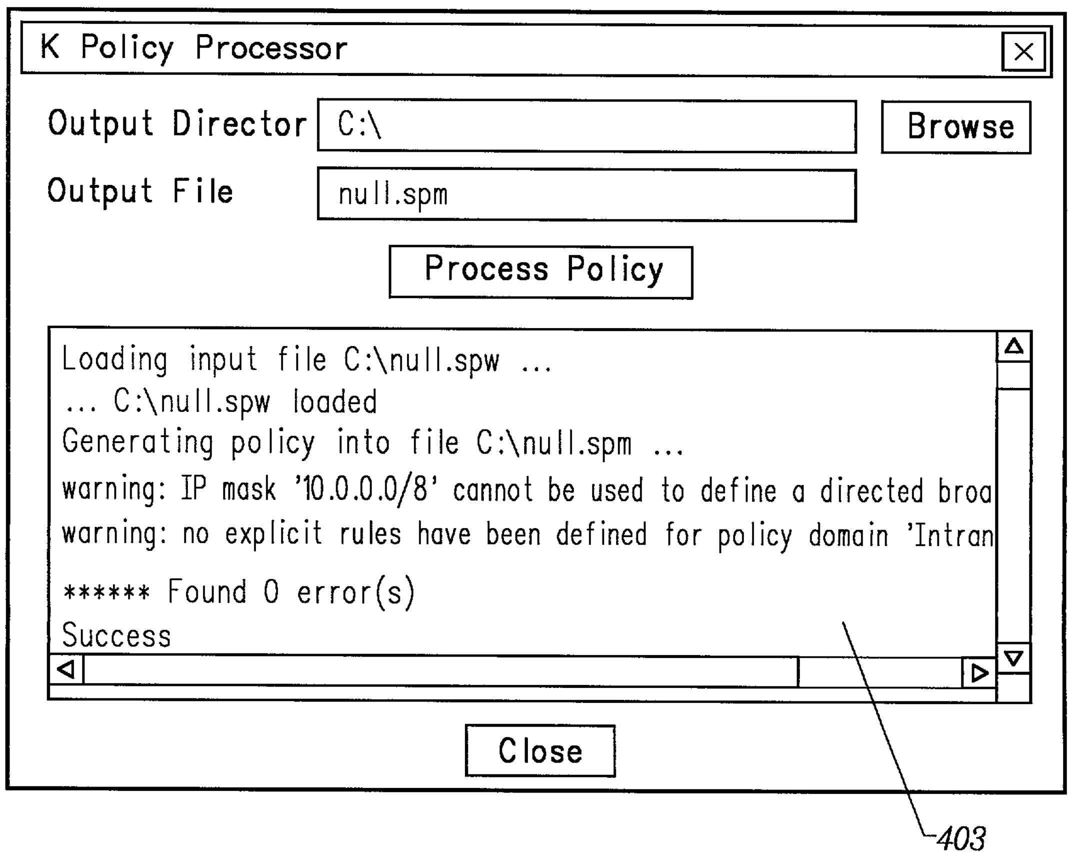


FIG. 4B

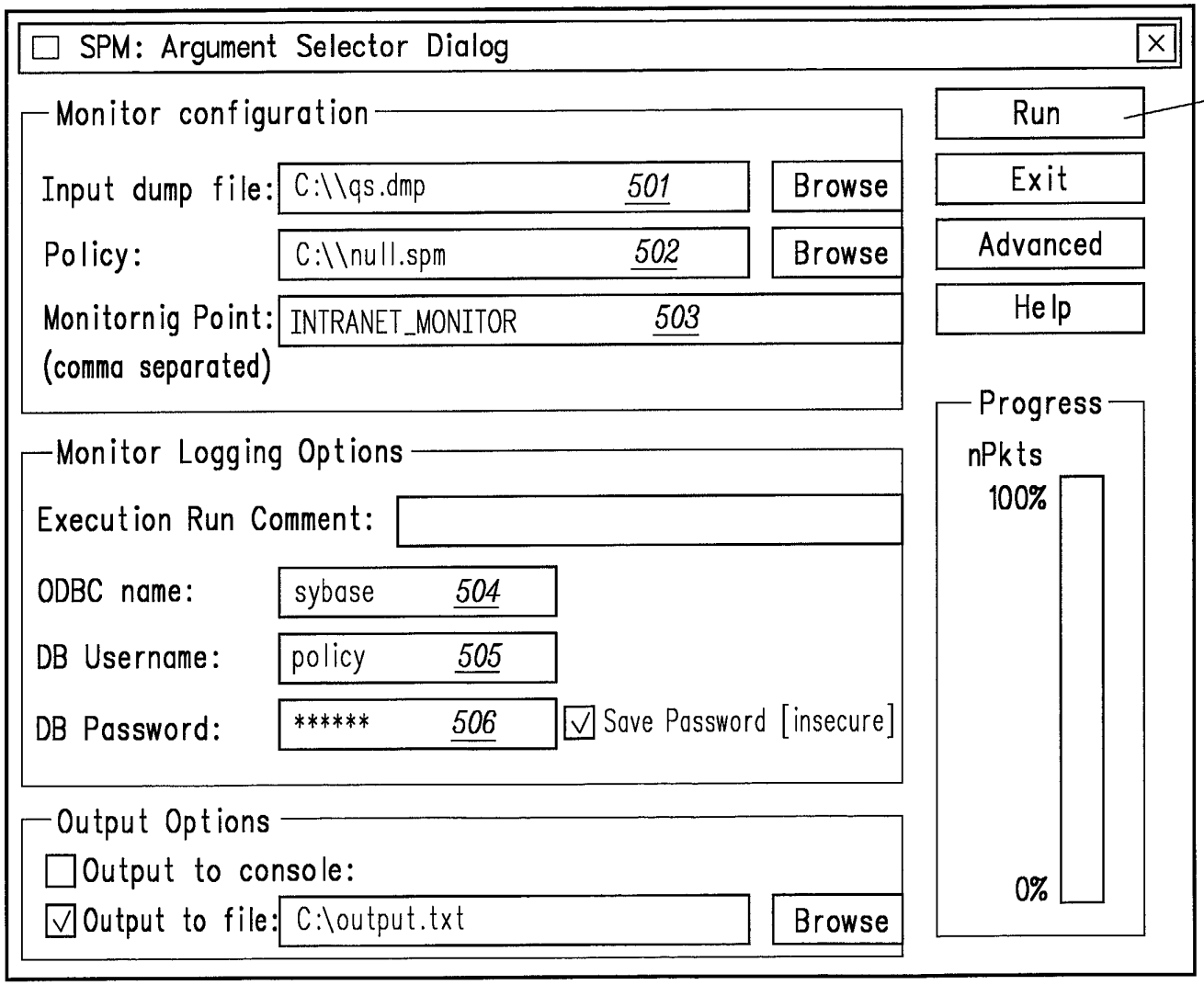

SPM: Argument Selector Dialog
Monitor configuration
Input dump file:
C:\\qs.dmp
501
Browse
Policy:
C:\\null.spm
502
Browse
Monitornig Point:
INTRANET_MONITOR
503
(comma separated)
Monitor Logging Options
Execution Run Comment:
ODBC name:
sybase
504
DB Username:
policy
505
DB Password:
******
506
Save Password [insecure]
Output Options
Output to console:
Output to file:
C:\output.txt
Browse
Run
507
Exit
Advanced
Help
Progress
nPkts
100%
0%

FIG. 5

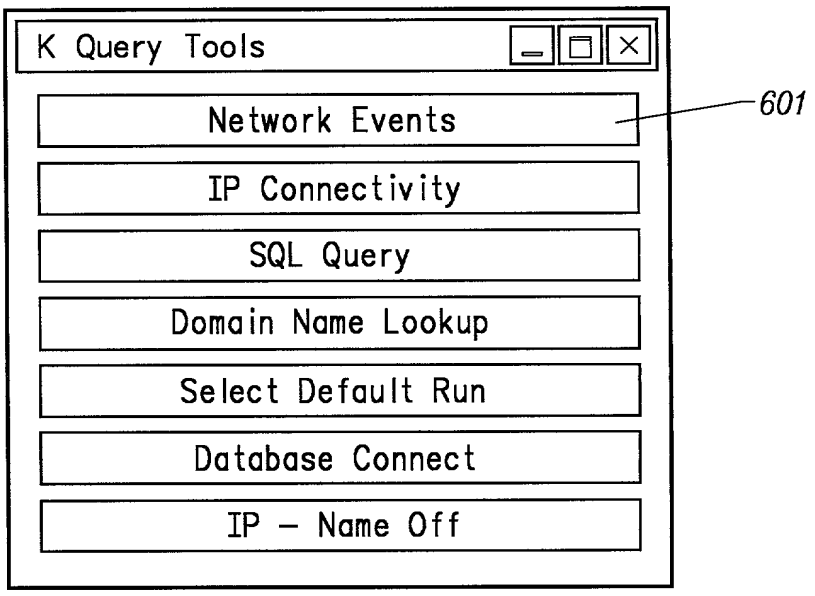

K Query Tools
Network Events
IP Connectivity
SQL Query
Domain Name Lookup
Select Default Run
Database Connect
IP – Name Off
601

FIG. 6

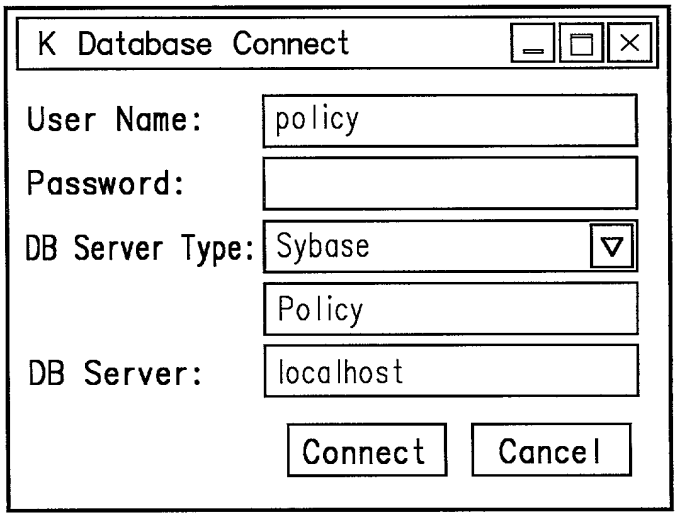

K Database Connect
User Name:
policy
Password:
DB Server Type:
Sybase
Policy
DB Server:
localhost
Connect
Cancel

FIG. 7

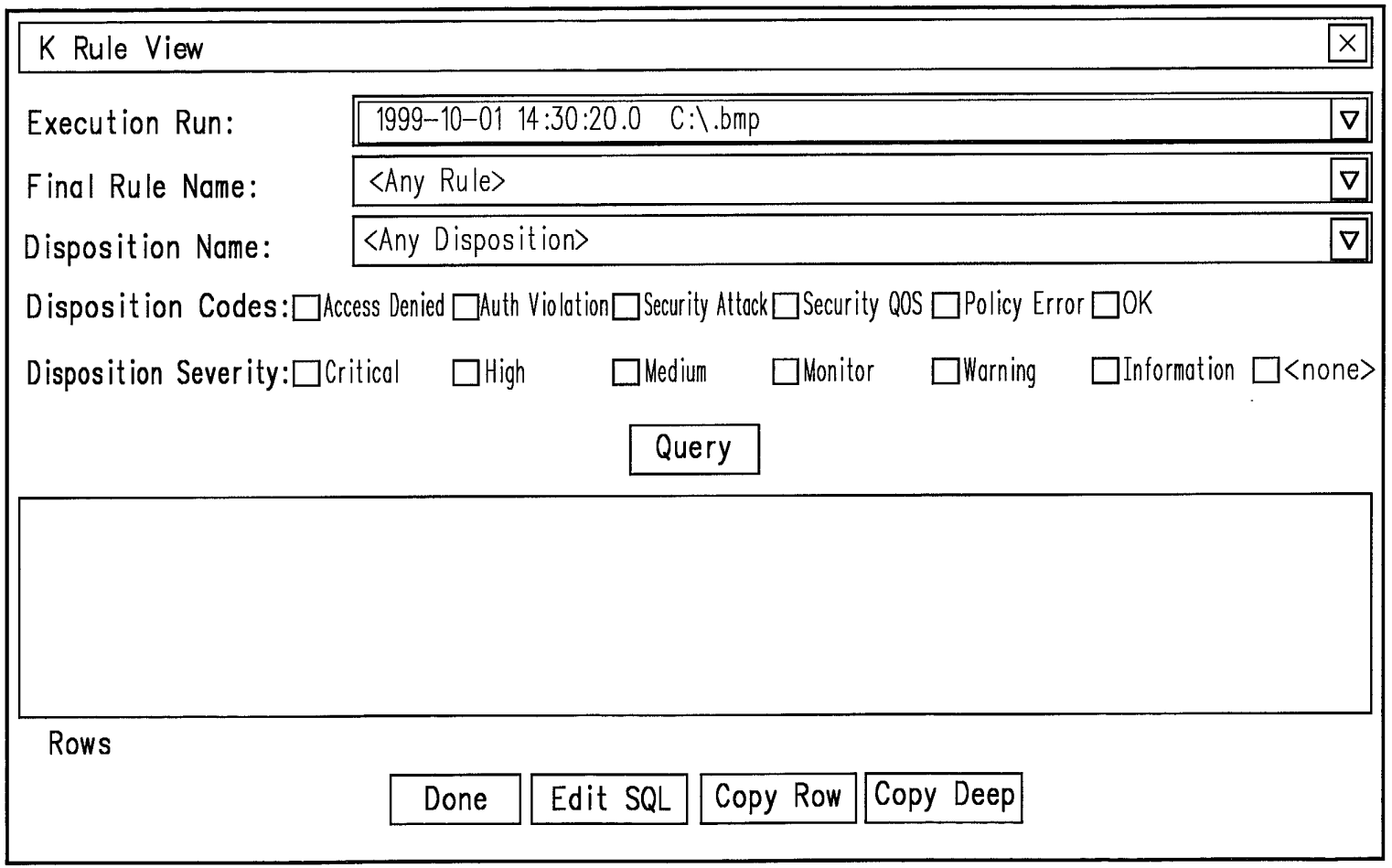

K Rule View
Execution Run:
1999-10-01 14:30:20.0 C:\.bmp
Final Rule Name:
<Any Rule>
Disposition Name:
<Any Disposition>
Disposition Codes:
Access Denied
Auth Violation
Security Attack
Security QOS
Policy Error
OK
Disposition Severity:
Critical
High
Medium
Monitor
Warning
Information
<none>
Query
Rows
Done
Edit SQL
Copy Row
Copy Deep

FIG. 8

K Rule View

Execution Run: 1999-10-01 14:30:20.0 C:\.bmp

Final Rule Name: <Any Rule>

Disposition Name: <Any Disposition>

Disposition Codes: ☐ Access Denied ☐ Auth Violation ☐ Security Attack ☐ Security QOS ☐ Policy Error ☐ OK

Disposition Severity: ☐ Critical ☐ High ☐ Medium ☐ Monitor ☐ Warning ☐ Information ☐ <none>

Query

Rule Name	Disposition Name	Initiator IP	Init Name	Target IP	Targ Name	Targ Service
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.198		http
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.201		http
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.198		http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	204.71.200.68	www3.yahoo.com	http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.97	kabale.securify.com	http
Tcp_Missed_Connections	Warn_Missed_Tcp_Connect	10.5.63.143	vg-143.securify.com	10.5.63.24	fred.securify.com	netbios-ssn

Rows 10

Done | Edit SQL | Copy Row | Copy Deep

FIG. 9

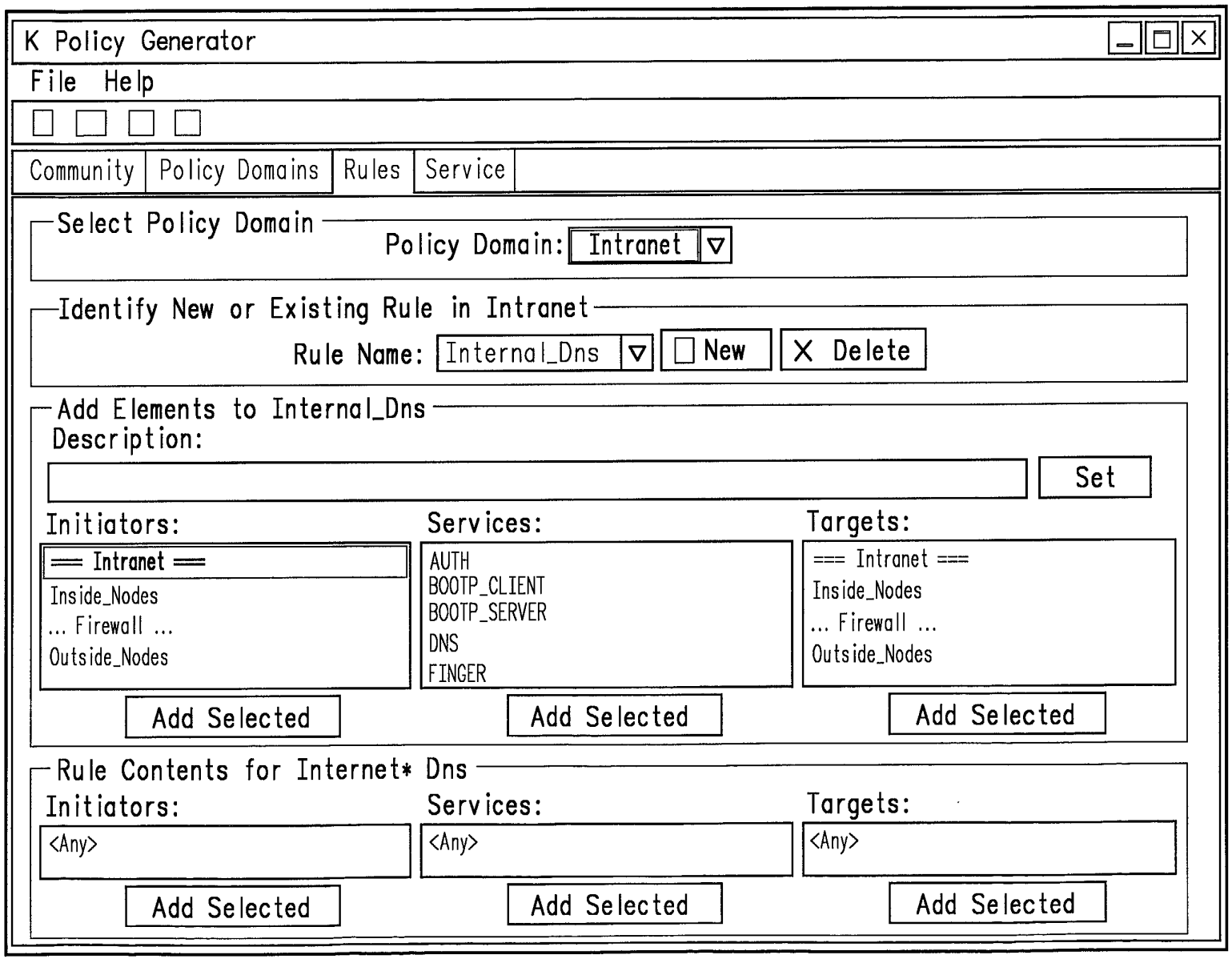

K Policy Generator
File Help
Community
Policy Domains
Rules
Service
Select Policy Domain
Policy Domain: Intranet
Identify New or Existing Rule in Intranet
Rule Name: Internal_Dns
New
Delete
Add Elements to Internal_Dns
Description:
Set
Initiators:
Services:
Targets:
== Intranet ==
Inside_Nodes
... Firewall ...
Outside_Nodes
AUTH
BOOTP_CLIENT
BOOTP_SERVER
DNS
FINGER
=== Intranet ===
Inside_Nodes
... Firewall ...
Outside_Nodes
Add Selected
Add Selected
Add Selected
Rule Contents for Internet* Dns
Initiators:
Services:
Targets:
<Any>
<Any>
<Any>
Add Selected
Add Selected
Add Selected

FIG. 10A

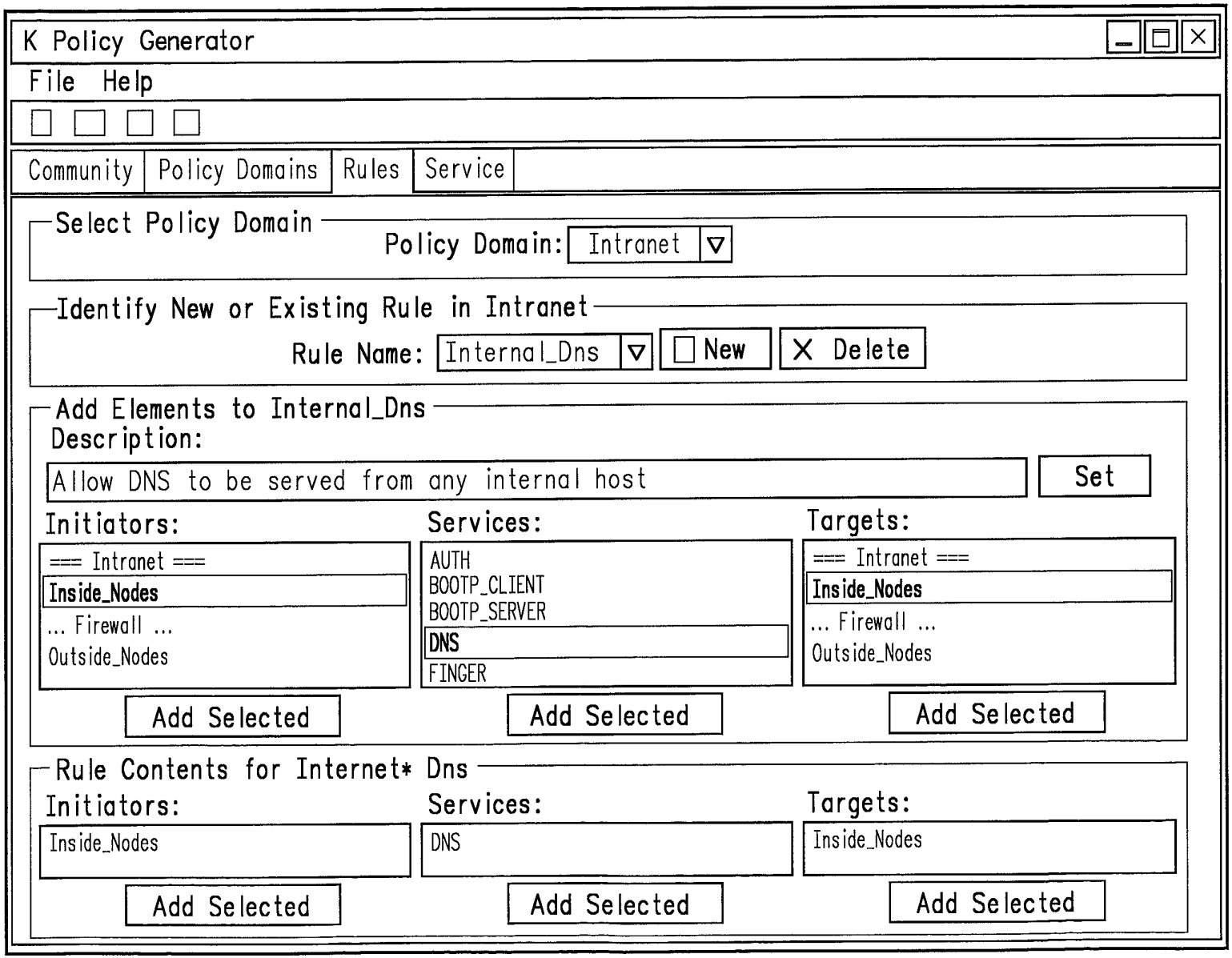

K Policy Generator
File Help
Community
Policy Domains
Rules
Service
Select Policy Domain
Policy Domain: Intranet
Identify New or Existing Rule in Intranet
Rule Name: Internal_Dns
New
Delete
Add Elements to Internal_Dns
Description:
Allow DNS to be served from any internal host
Set
Initiators:
Services:
Targets:
=== Intranet ===
Inside_Nodes
... Firewall ...
Outside_Nodes
AUTH
BOOTP_CLIENT
BOOTP_SERVER
DNS
FINGER
Add Selected
Rule Contents for Internet* Dns
Inside_Nodes
DNS

FIG. 10B

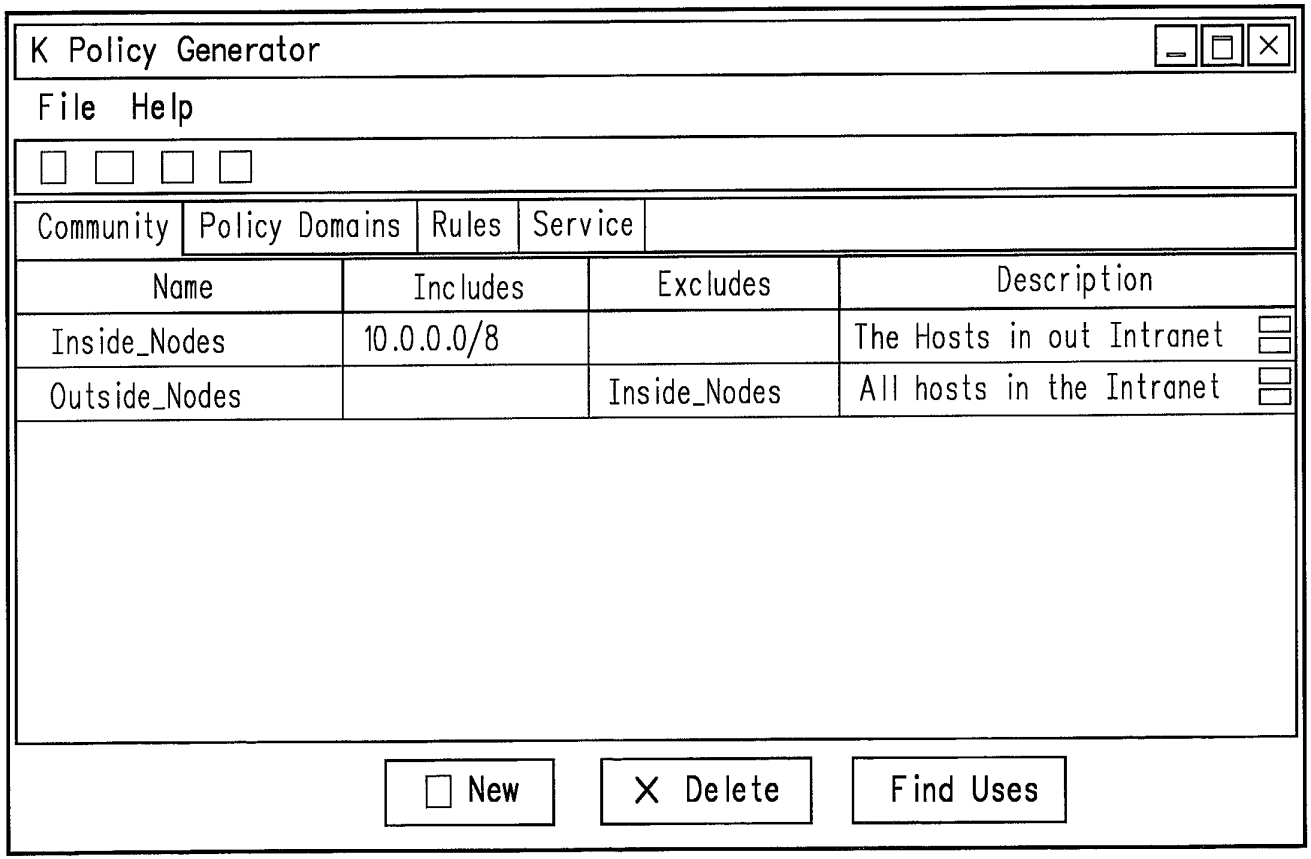

K Policy Generator
File Help
Community
Policy Domains
Rules
Service
Name
Includes
Excludes
Description
Inside_Nodes
10.0.0.0/8
The Hosts in out Intranet
Outside_Nodes
Inside_Nodes
All hosts in the Intranet
New
Delete
Find Uses

FIG. 10C

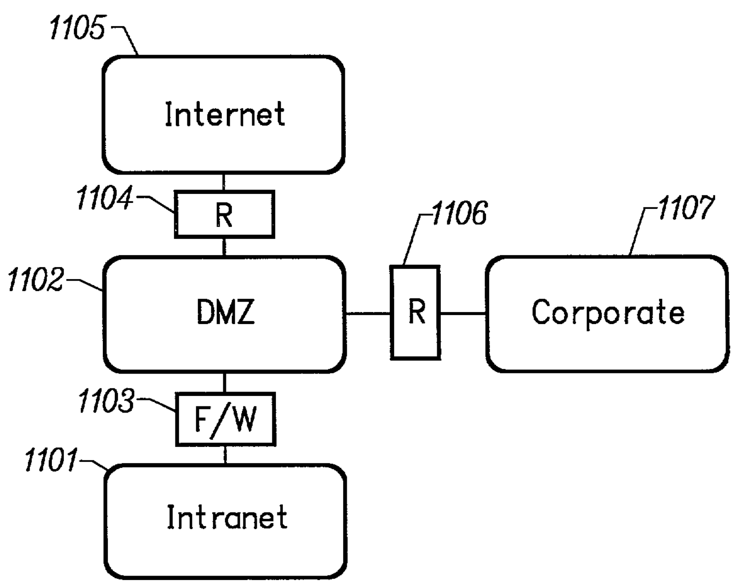


FIG. 11

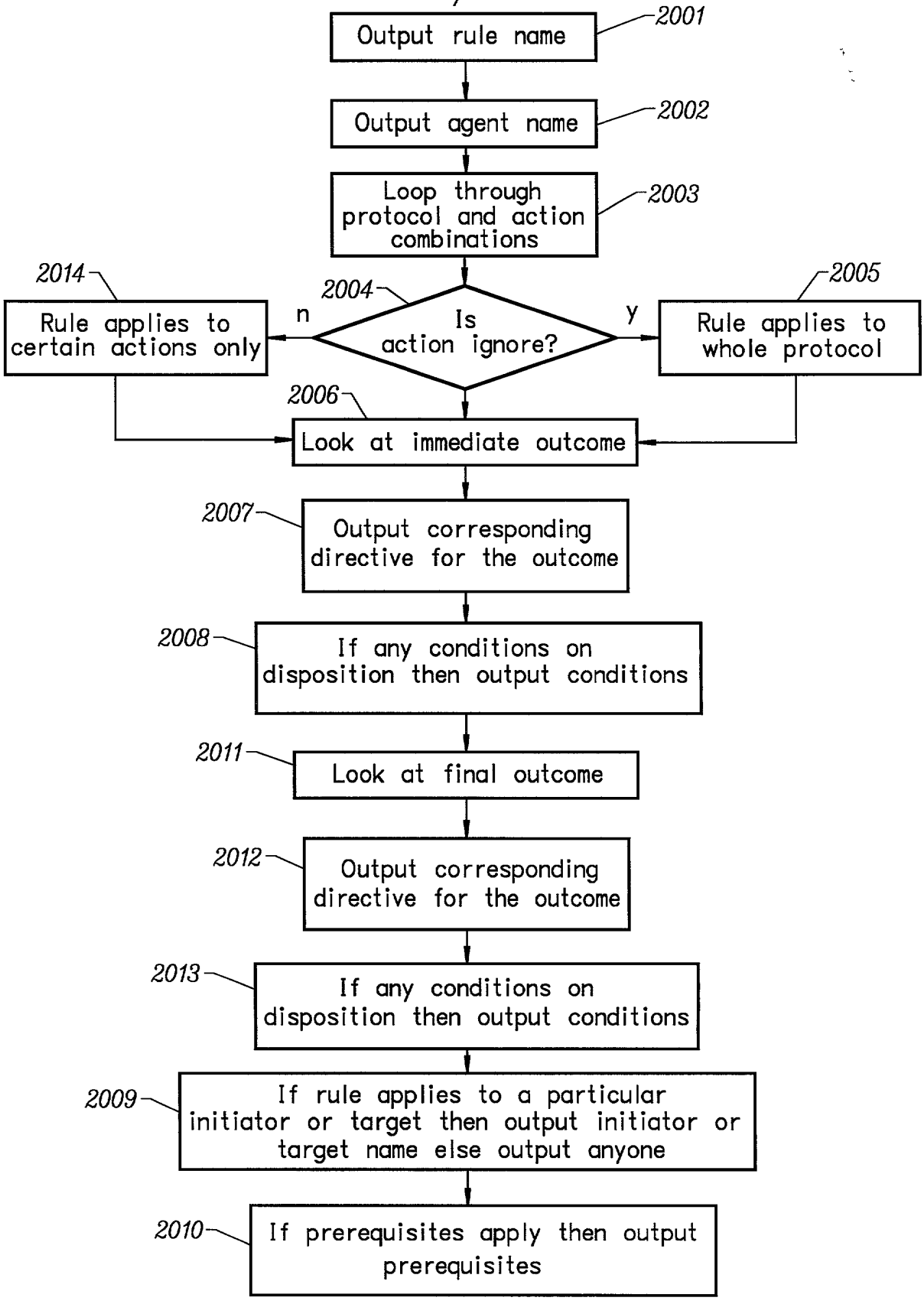


FIG. 12

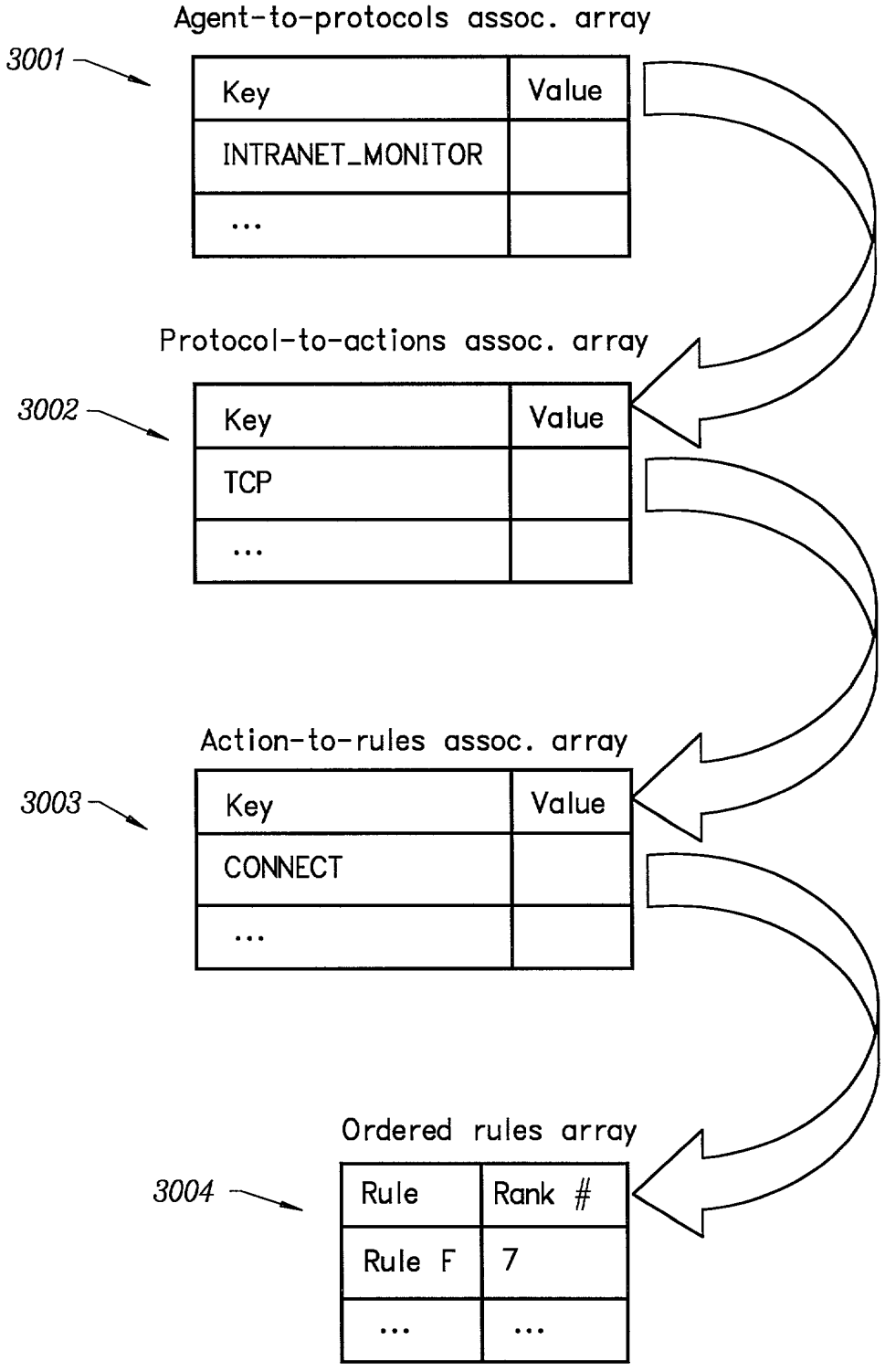

Agent-to-protocols assoc. array
3001
Key
Value
INTRANET_MONITOR
...
Protocol-to-actions assoc. array
3002
Key
Value
TCP
...
Action-to-rules assoc. array
3003
Key
Value
CONNECT
...
Ordered rules array
3004
Rule
Rank #
Rule F
7
...
...

FIG. 13

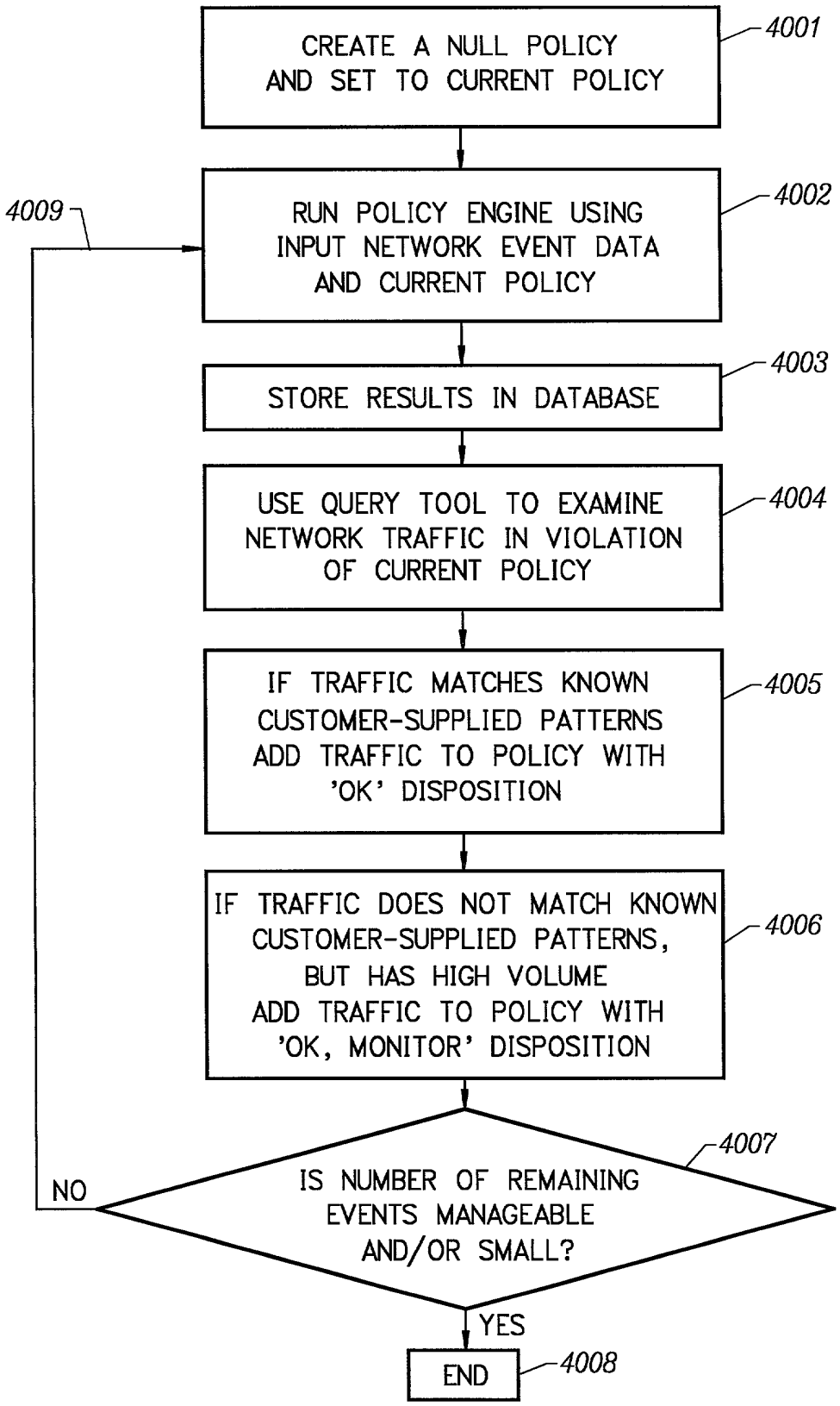

CREATE A NULL POLICY AND SET TO CURRENT POLICY
4001
RUN POLICY ENGINE USING INPUT NETWORK EVENT DATA AND CURRENT POLICY
4002
4009
STORE RESULTS IN DATABASE
4003
USE QUERY TOOL TO EXAMINE NETWORK TRAFFIC IN VIOLATION OF CURRENT POLICY
4004
IF TRAFFIC MATCHES KNOWN CUSTOMER-SUPPLIED PATTERNS ADD TRAFFIC TO POLICY WITH 'OK' DISPOSITION
4005
IF TRAFFIC DOES NOT MATCH KNOWN CUSTOMER-SUPPLIED PATTERNS, BUT HAS HIGH VOLUME ADD TRAFFIC TO POLICY WITH 'OK, MONITOR' DISPOSITION
4006
IS NUMBER OF REMAINING EVENTS MANAGEABLE AND/OR SMALL?
4007
NO
YES
END
4008

FIG. 14

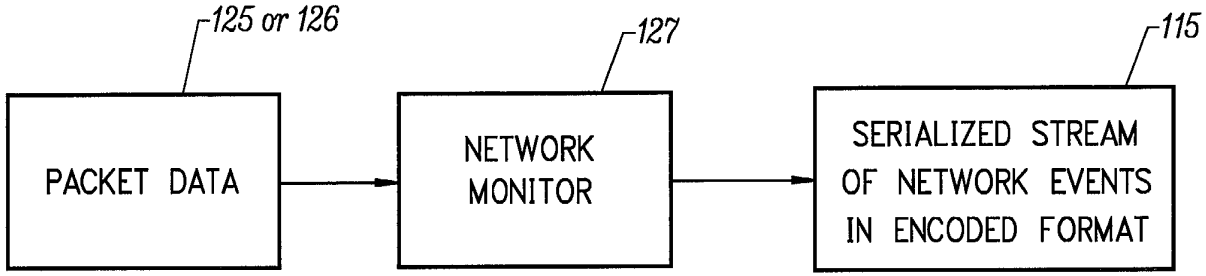

125 or 126
127
115
PACKET DATA
NETWORK MONITOR
SERIALIZED STREAM OF NETWORK EVENTS IN ENCODED FORMAT

FIG. 15

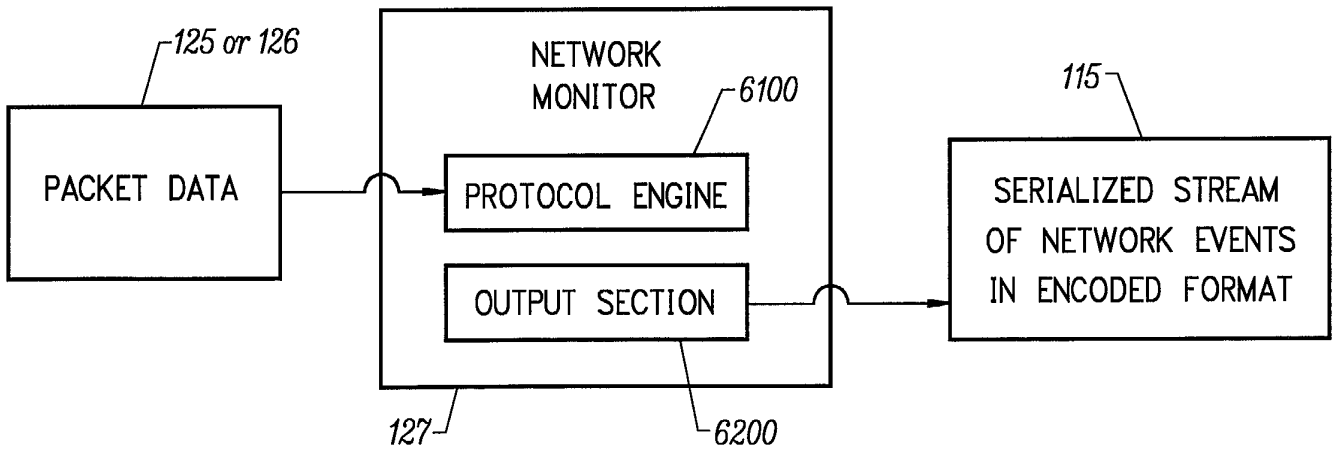

125 or 126
NETWORK MONITOR
6100
115
PACKET DATA
PROTOCOL ENGINE
OUTPUT SECTION
SERIALIZED STREAM OF NETWORK EVENTS IN ENCODED FORMAT
127
6200

FIG. 16

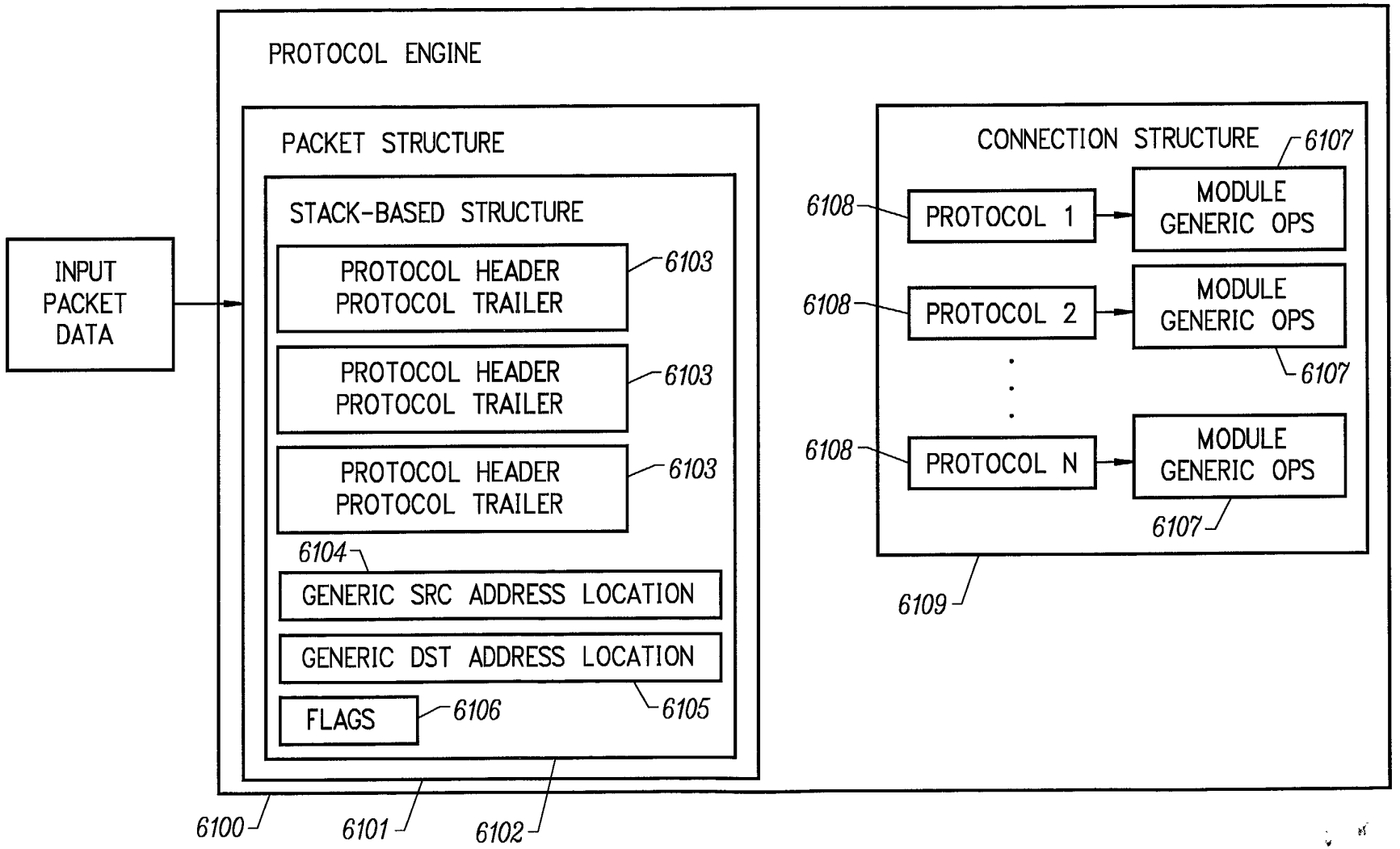

PROTOCOL ENGINE
PACKET STRUCTURE
STACK-BASED STRUCTURE
INPUT PACKET DATA
PROTOCOL HEADER PROTOCOL TRAILER
6103
PROTOCOL HEADER PROTOCOL TRAILER
6103
PROTOCOL HEADER PROTOCOL TRAILER
6103
6104
GENERIC SRC ADDRESS LOCATION
GENERIC DST ADDRESS LOCATION
6105
FLAGS
6106
CONNECTION STRUCTURE
6107
6108
PROTOCOL 1
MODULE GENERIC OPS
6108
PROTOCOL 2
MODULE GENERIC OPS
6107
6108
PROTOCOL N
MODULE GENERIC OPS
6107
6109
6100
6101
6102

FIG. 17

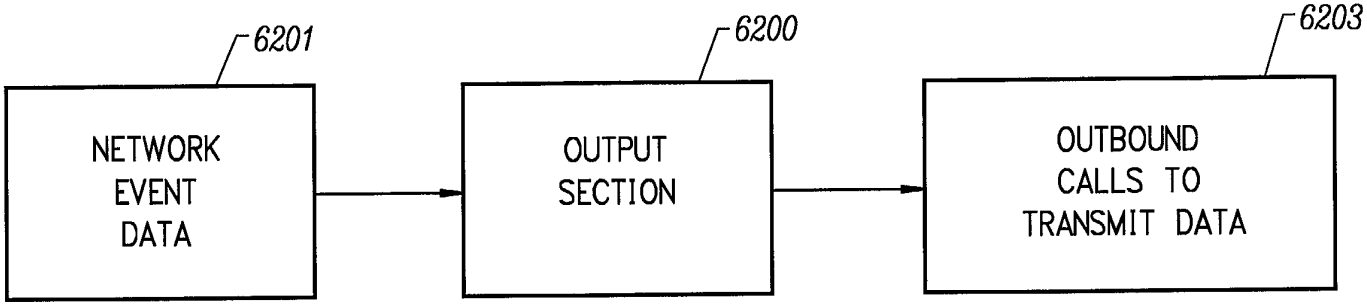

6201
6200
6203
NETWORK EVENT DATA
OUTPUT SECTION
OUTBOUND CALLS TO TRANSMIT DATA

FIG. 18

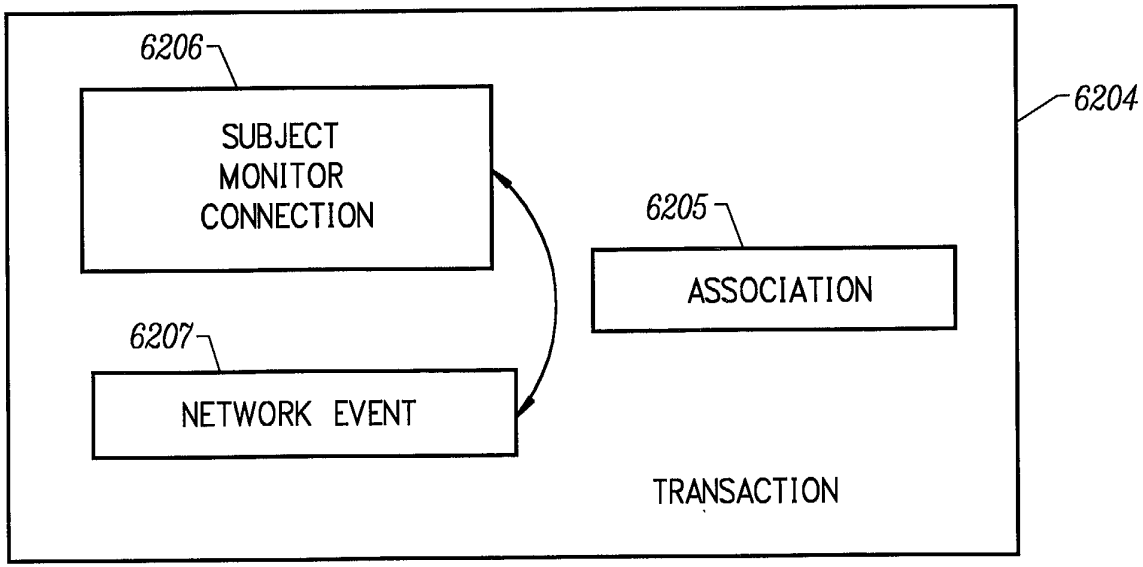

6206
6204
SUBJECT MONITOR CONNECTION
6205
ASSOCIATION
6207
NETWORK EVENT
TRANSACTION

FIG. 19

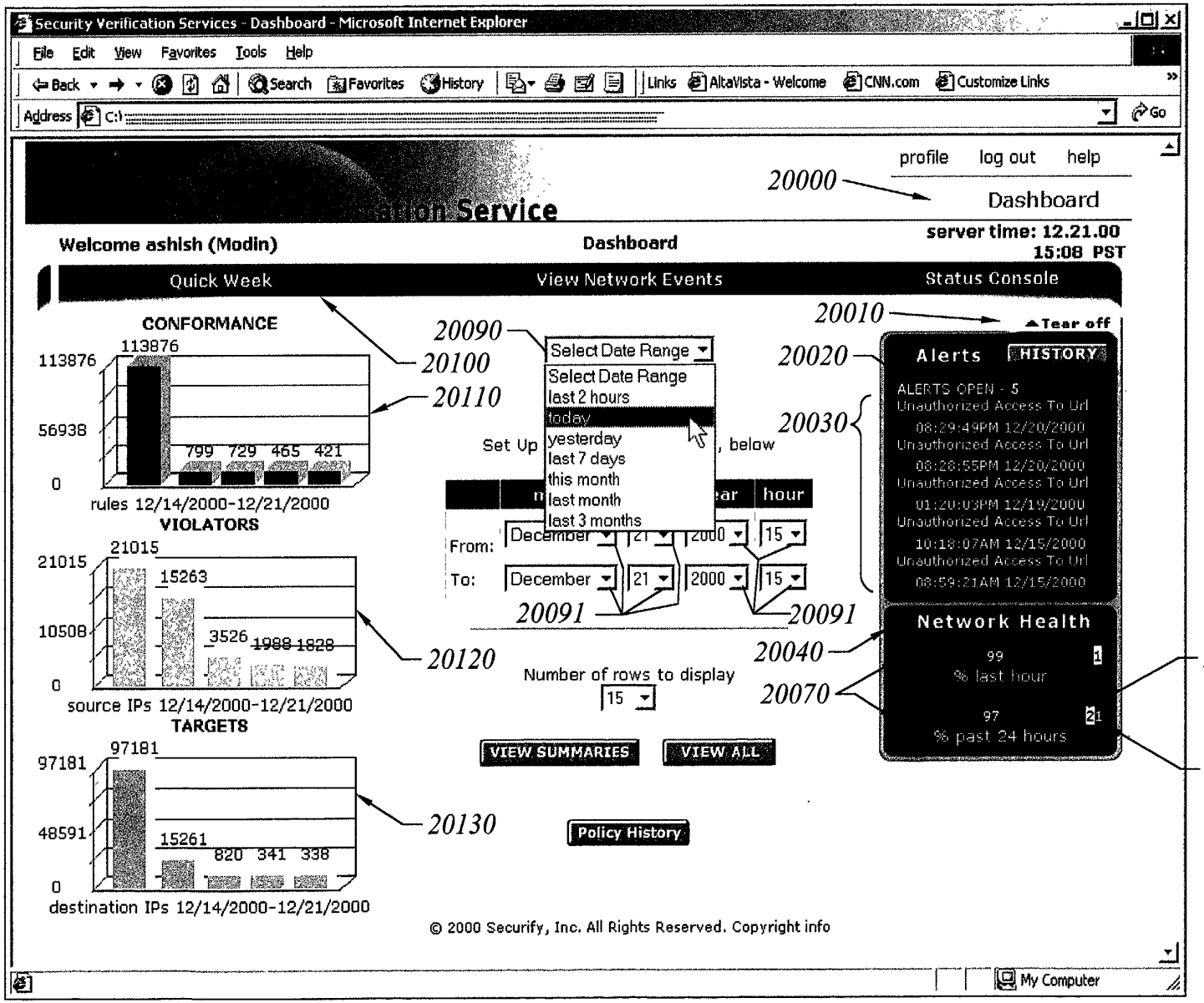

Security Verification Services - Dashboard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links
Address C:\
Go
profile log out help
20000
Dashboard
Welcome ashish (Modin)
Dashboard
server time: 12.21.00
15:08 PST
Quick Week
View Network Events
Status Console
20010
Tear off
CONFORMANCE
113876
56938
0
799 729 465 421
rules 12/14/2000-12/21/2000
20100
20110
20090
Select Date Range
Select Date Range
last 2 hours
today
yesterday
last 7 days
this month
last month
last 3 months
Set Up , below
hour
From: December 21 2000 15
To: December 21 2000 15
20091
20091
20020
Alerts
HISTORY
ALERTS OPEN - 5
Unauthorized Access To Url
08:29:49PM 12/20/2000
Unauthorized Access To Url
08:28:55PM 12/20/2000
Unauthorized Access To Url
01:20:03PM 12/19/2000
Unauthorized Access To Url
10:18:07AM 12/15/2000
Unauthorized Access To Url
08:59:21AM 12/15/2000
20030
VIOLATORS
21015
10508
0
15263
3526
source IPs 12/14/2000-12/21/2000
20120
Number of rows to display
15
20040
Network Health
99
1
% last hour
97
21
% past 24 hours
20060
20070
20050
VIEW SUMMARIES
VIEW ALL
TARGETS
97181
48591
0
15261
820 341 338
destination IPs 12/14/2000-12/21/2000
20130
Policy History
© 2000 Securify, Inc. All Rights Reserved. Copyright info
My Computer

FIG. 20

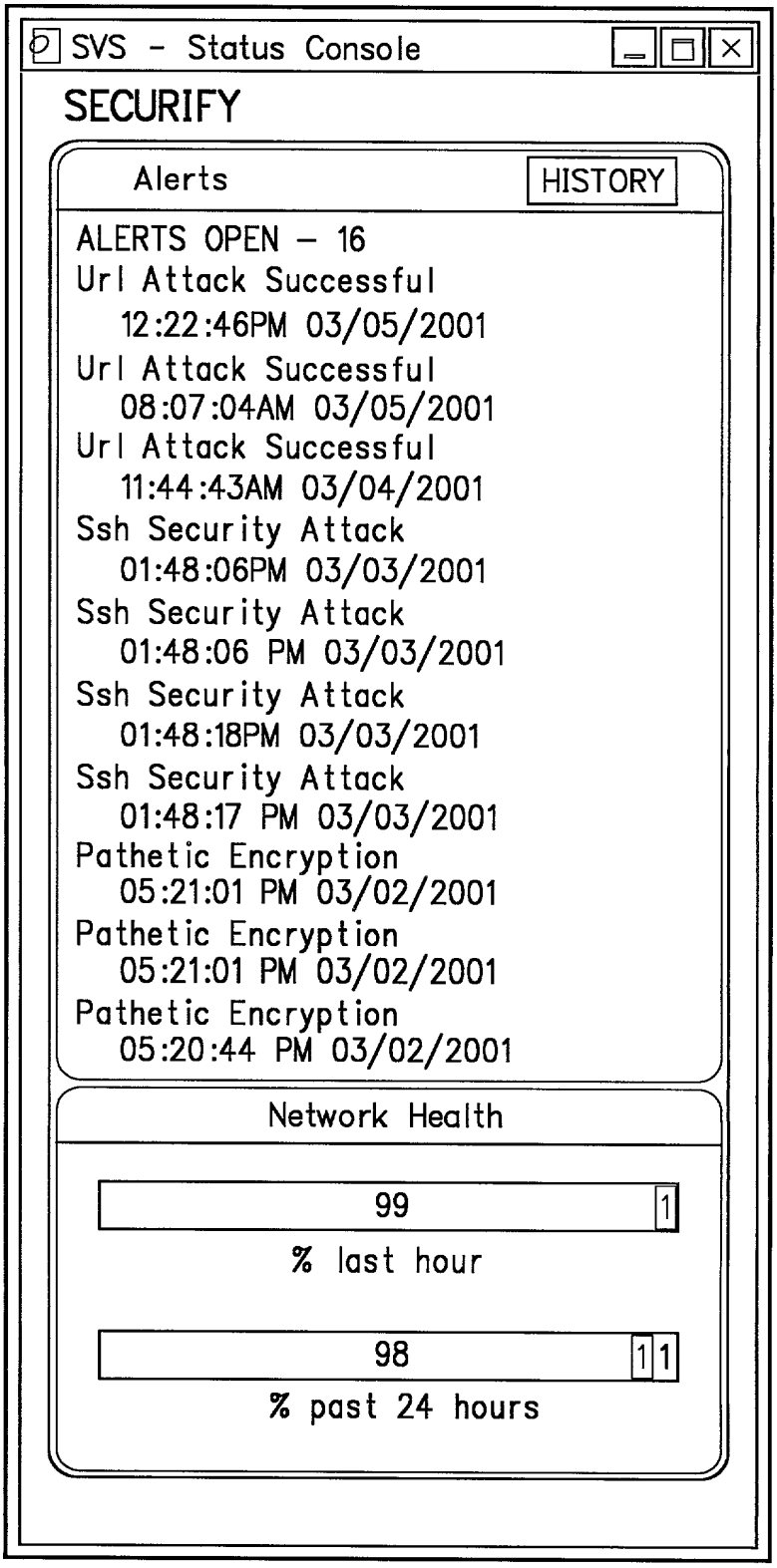
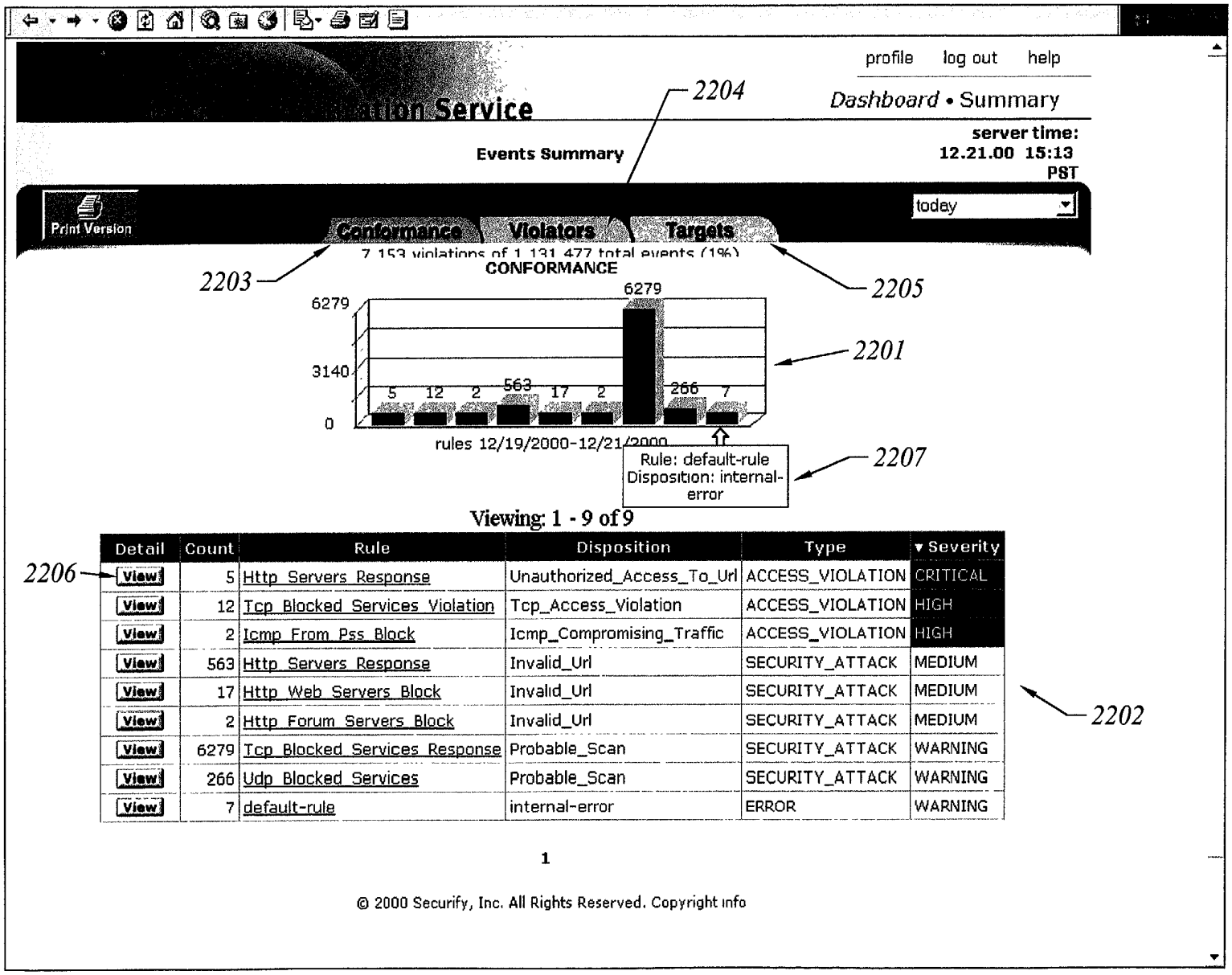


FIG. 21



Viewing: 1 - 9 of 9

Detail	Count	Rule	Disposition	Type	▾ Severity
View	5	Http_Servers_Response	Unauthorized_Access_To_Url	ACCESS_VIOLATION	CRITICAL
View	12	Tcp_Blocked_Services_Violation	Tcp_Access_Violation	ACCESS_VIOLATION	HIGH
View	2	Icmp_From_Pss_Block	Icmp_Compromising_Traffic	ACCESS_VIOLATION	HIGH
View	563	Http_Servers_Response	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	17	Http_Web_Servers_Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	2	Http_Forum_Servers_Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	6279	Tcp_Blocked_Services_Response	Probable_Scan	SECURITY_ATTACK	WARNING
View	266	Udp_Blocked_Services	Probable_Scan	SECURITY_ATTACK	WARNING
View	7	default-rule	internal-error	ERROR	WARNING

1

FIG. 22

profile log out help

Dashboard • *Summary* • Detail

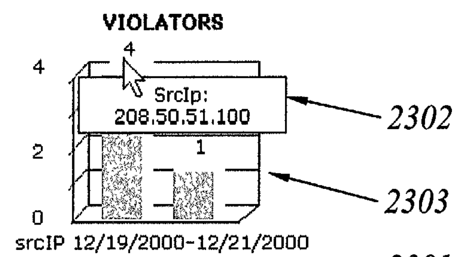
Service

Conformance Event Detail **server time: 12.21.00 17:24 PST**

Print Version

Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL

today



2301

Viewing: 1 - 5 of 5

Detail	▼SrcIP	SrcPort	DstIp	DstPort	ProtId	DateTime	AppData	Status	Monitor
View	212.210.11.4	2135	209.143.242.119	80	6	09:36:35AM 12/21/2000	209.143.242.119:80/	200	PSS MONITOR
View	208.50.51.100	1060	209.143.242.118	80	6	08:28:55PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1062	209.143.242.118	80	6	08:29:49PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1064	209.143.242.118	80	6	08:30:15PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1066	209.143.242.118	80	6	08:30:38PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR

1

FIG. 23

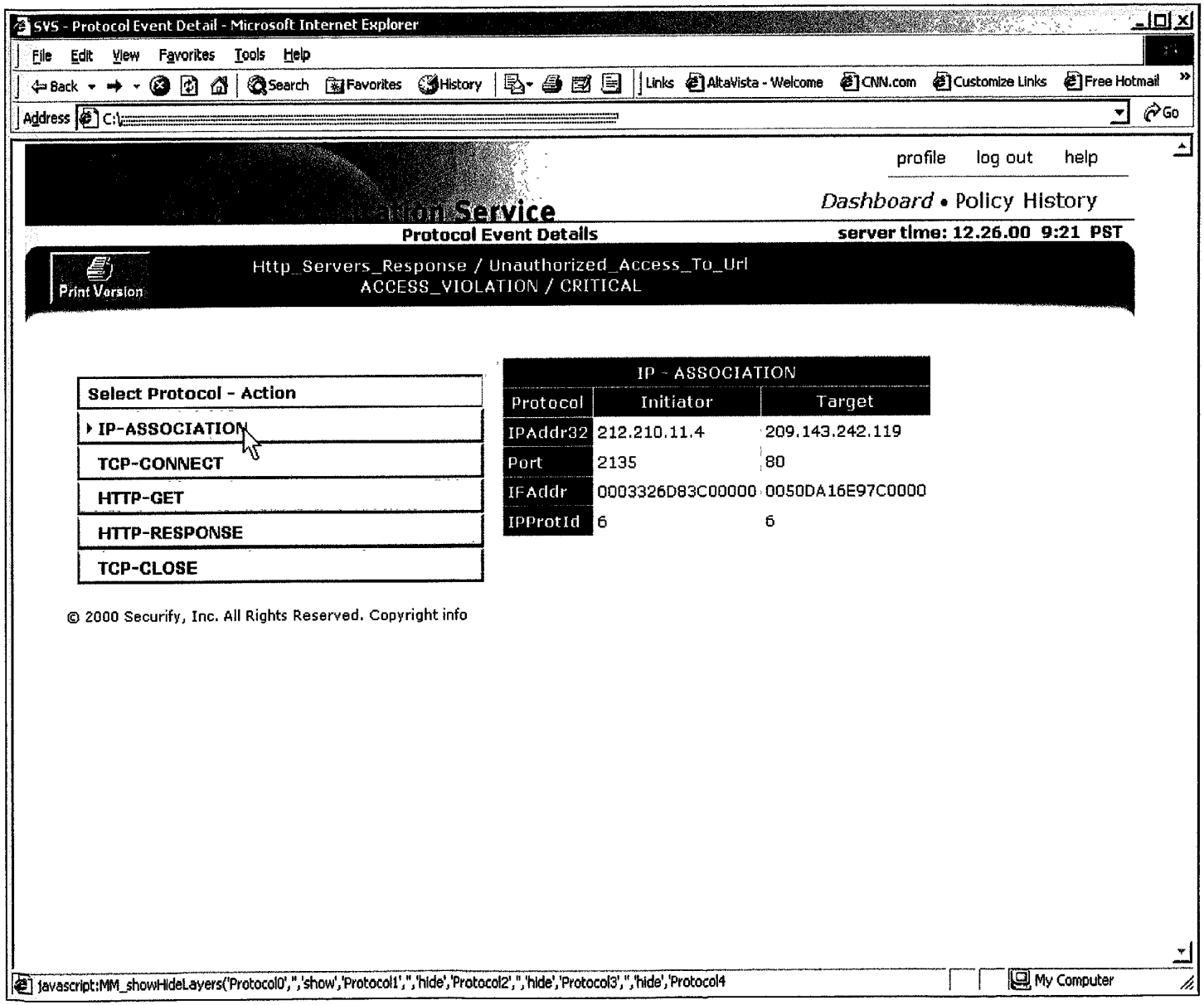

SVS - Protocol Event Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links Free Hotmail
Address C:\
Go
profile log out help
Dashboard • Policy History
Protocol Event Details
server time: 12.26.00 9:21 PST
Print Version
Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL
Select Protocol - Action
IP-ASSOCIATION
TCP-CONNECT
HTTP-GET
HTTP-RESPONSE
TCP-CLOSE
IP - ASSOCIATION
Protocol Initiator Target
IPAddr32 212.210.11.4 209.143.242.119
Port 2135 80
IFAddr 0003326D83C00000 0050DA16E97C0000
IPProtId 6 6
© 2000 Securify, Inc. All Rights Reserved. Copyright info
javascript:MM_showHideLayers('Protocol0','','show','Protocol1','','hide','Protocol2','','hide','Protocol3','','hide','Protocol4
My Computer

FIG. 24

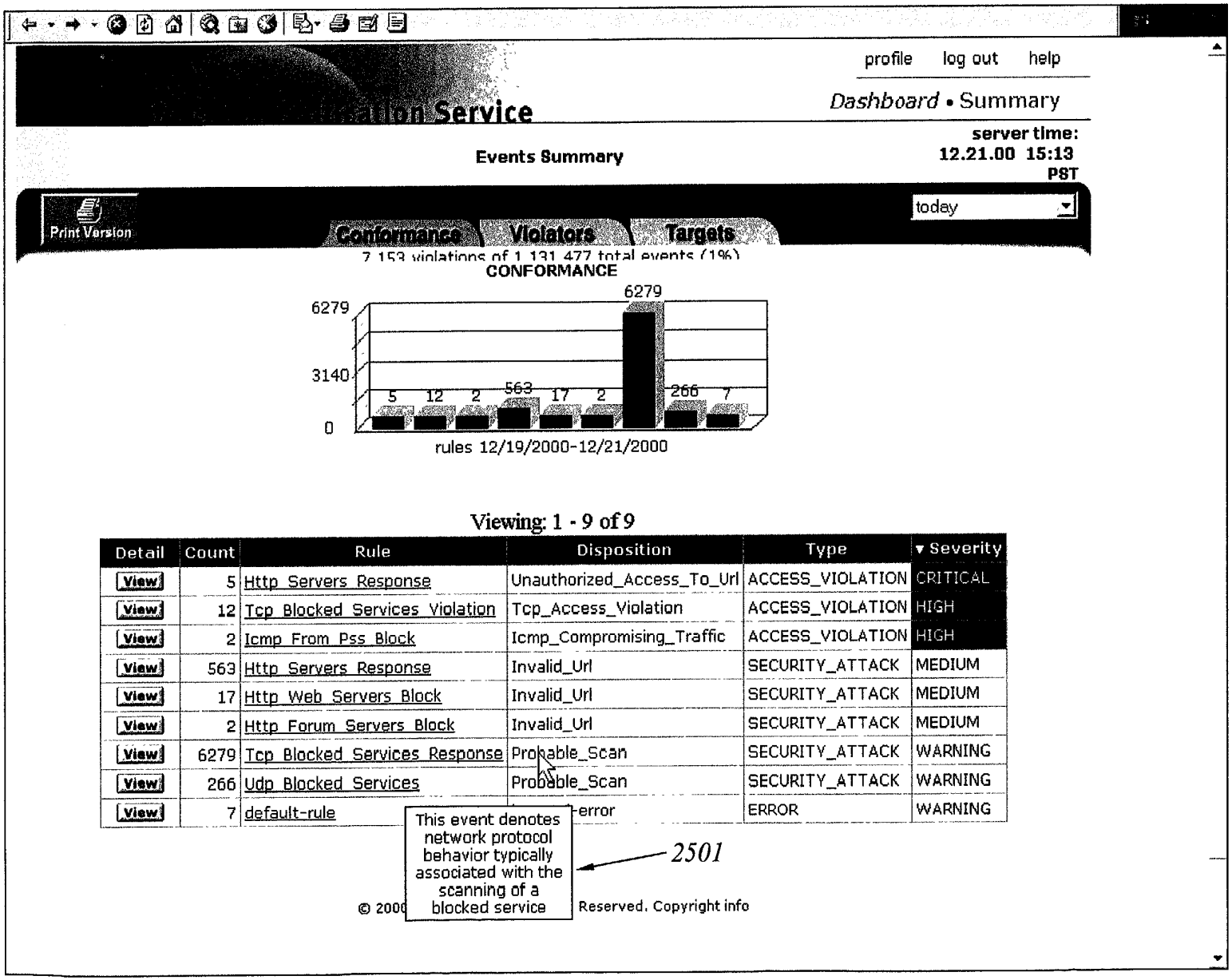

profile
log out
help
Dashboard • Summary
server time:
12.21.00 15:13
PST
Events Summary
Print Version
today
Conformance
Violators
Targets
CONFORMANCE
6279
3140
0
5
12
2
563
17
2
6279
266
7
rules 12/19/2000-12/21/2000
Viewing: 1 - 9 of 9
Detail
Count
Rule
Disposition
Type
Severity
View
5
Http_Servers_Response
Unauthorized_Access_To_Url
ACCESS_VIOLATION
CRITICAL
View
12
Tcp_Blocked_Services_Violation
Tcp_Access_Violation
ACCESS_VIOLATION
HIGH
View
2
Icmp_From_Pss_Block
Icmp_Compromising_Traffic
ACCESS_VIOLATION
HIGH
View
563
Http_Servers_Response
Invalid_Url
SECURITY_ATTACK
MEDIUM
View
17
Http_Web_Servers_Block
Invalid_Url
SECURITY_ATTACK
MEDIUM
View
2
Http_Forum_Servers_Block
Invalid_Url
SECURITY_ATTACK
MEDIUM
View
6279
Tcp_Blocked_Services_Response
Probable_Scan
SECURITY_ATTACK
WARNING
View
266
Udp_Blocked_Services
Probable_Scan
SECURITY_ATTACK
WARNING
View
7
default-rule
error
ERROR
WARNING
This event denotes network protocol behavior typically associated with the scanning of a blocked service
2501
Reserved. Copyright info

FIG. 25

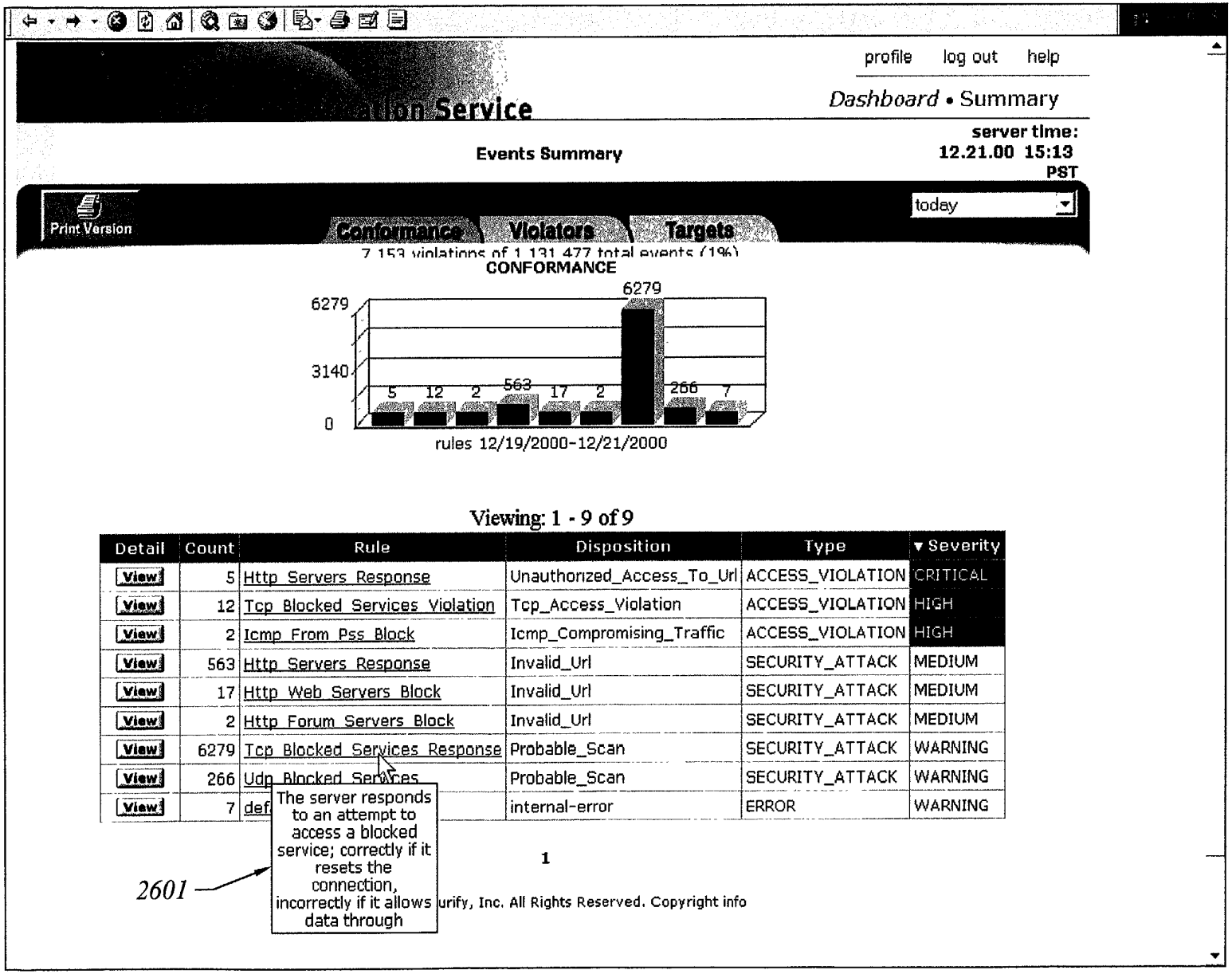

profile
log out
help
Dashboard • Summary
Service
server time:
12.21.00 15:13
PST
Events Summary
Print Version
today
Conformance
Violators
Targets
7,159 violations of 1,131,477 total events (1%)
CONFORMANCE
6279
3140
0
5
12
2
563
17
2
6279
266
7
rules 12/19/2000-12/21/2000
Viewing: 1 - 9 of 9
Detail
Count
Rule
Disposition
Type
▼ Severity
View
5
Http_Servers_Response
Unauthorized_Access_To_Url
ACCESS_VIOLATION
CRITICAL
View
12
Tcp_Blocked_Services_Violation
Tcp_Access_Violation
ACCESS_VIOLATION
HIGH
View
2
Icmp_From_Pss_Block
Icmp_Compromising_Traffic
ACCESS_VIOLATION
HIGH
View
563
Http_Servers_Response
Invalid_Url
SECURITY_ATTACK
MEDIUM
View
17
Http_Web_Servers_Block
Invalid_Url
SECURITY_ATTACK
MEDIUM
View
2
Http_Forum_Servers_Block
Invalid_Url
SECURITY_ATTACK
MEDIUM
View
6279
Tcp_Blocked_Services_Response
Probable_Scan
SECURITY_ATTACK
WARNING
View
266
Udp_Blocked_Services
Probable_Scan
SECURITY_ATTACK
WARNING
View
7
def
internal-error
ERROR
WARNING
The server responds to an attempt to access a blocked service; correctly if it resets the connection, incorrectly if it allows data through
2601
1
urify, Inc. All Rights Reserved. Copyright info

FIG. 26

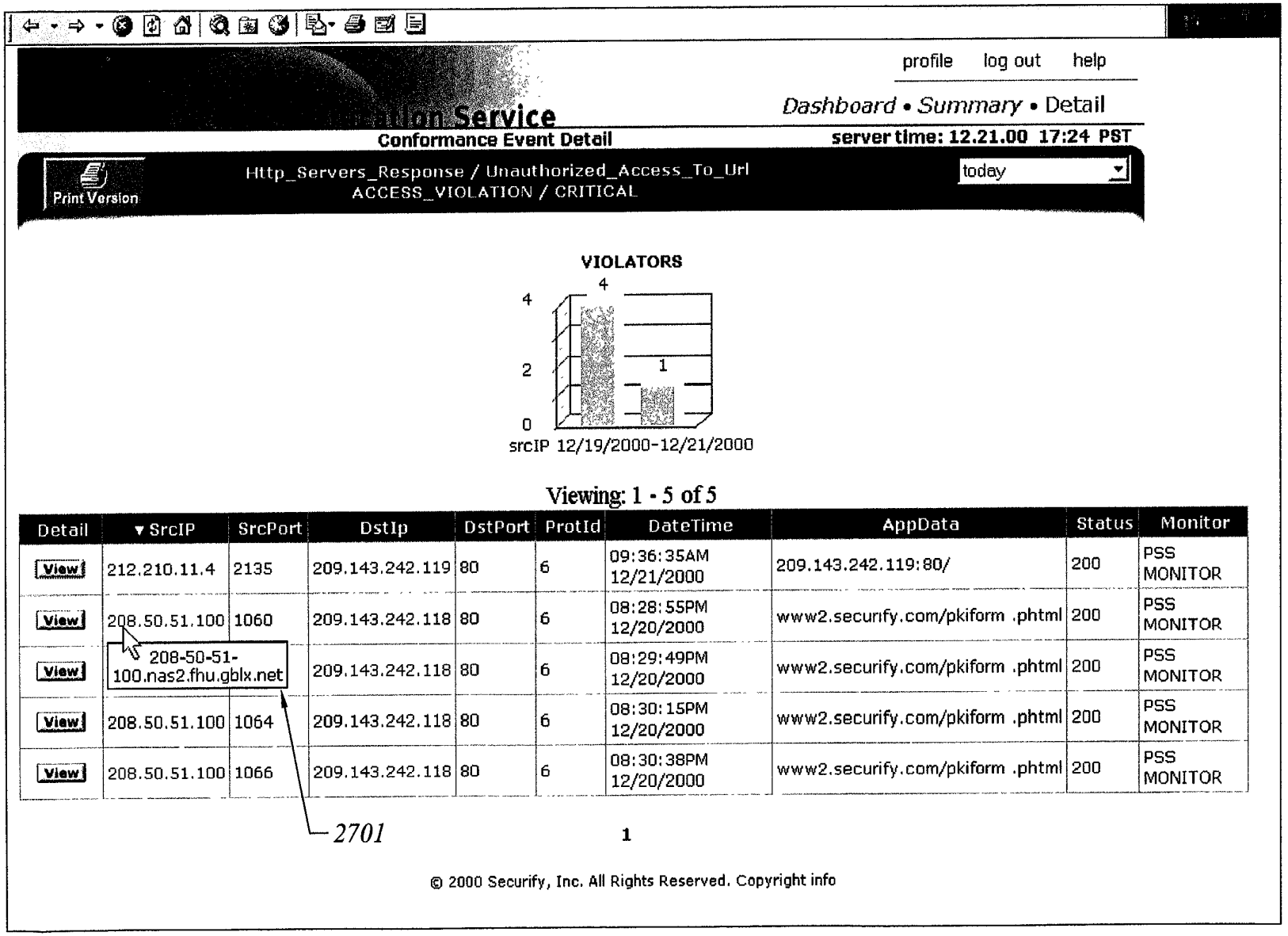

profile
log out
help
Dashboard • Summary • Detail
Conformance Event Detail
server time: 12.21.00 17:24 PST
Print Version
Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL
today
VIOLATORS
4
2
0
4
1
srcIP 12/19/2000-12/21/2000
Viewing: 1 - 5 of 5
Detail
▼ SrcIP
SrcPort
DstIp
DstPort
ProtId
DateTime
AppData
Status
Monitor
View
212.210.11.4
2135
209.143.242.119
80
6
09:36:35AM 12/21/2000
209.143.242.119:80/
200
PSS MONITOR
View
208.50.51.100
1060
209.143.242.118
80
6
08:28:55PM 12/20/2000
www2.securify.com/pkiform .phtml
200
PSS MONITOR
View
208-50-51-100.nas2.fhu.gblx.net
209.143.242.118
80
6
08:29:49PM 12/20/2000
www2.securify.com/pkiform .phtml
200
PSS MONITOR
View
208.50.51.100
1064
209.143.242.118
80
6
08:30:15PM 12/20/2000
www2.securify.com/pkiform .phtml
200
PSS MONITOR
View
208.50.51.100
1066
209.143.242.118
80
6
08:30:38PM 12/20/2000
www2.securify.com/pkiform .phtml
200
PSS MONITOR
2701
1
© 2000 Securify, Inc. All Rights Reserved. Copyright info

FIG. 27

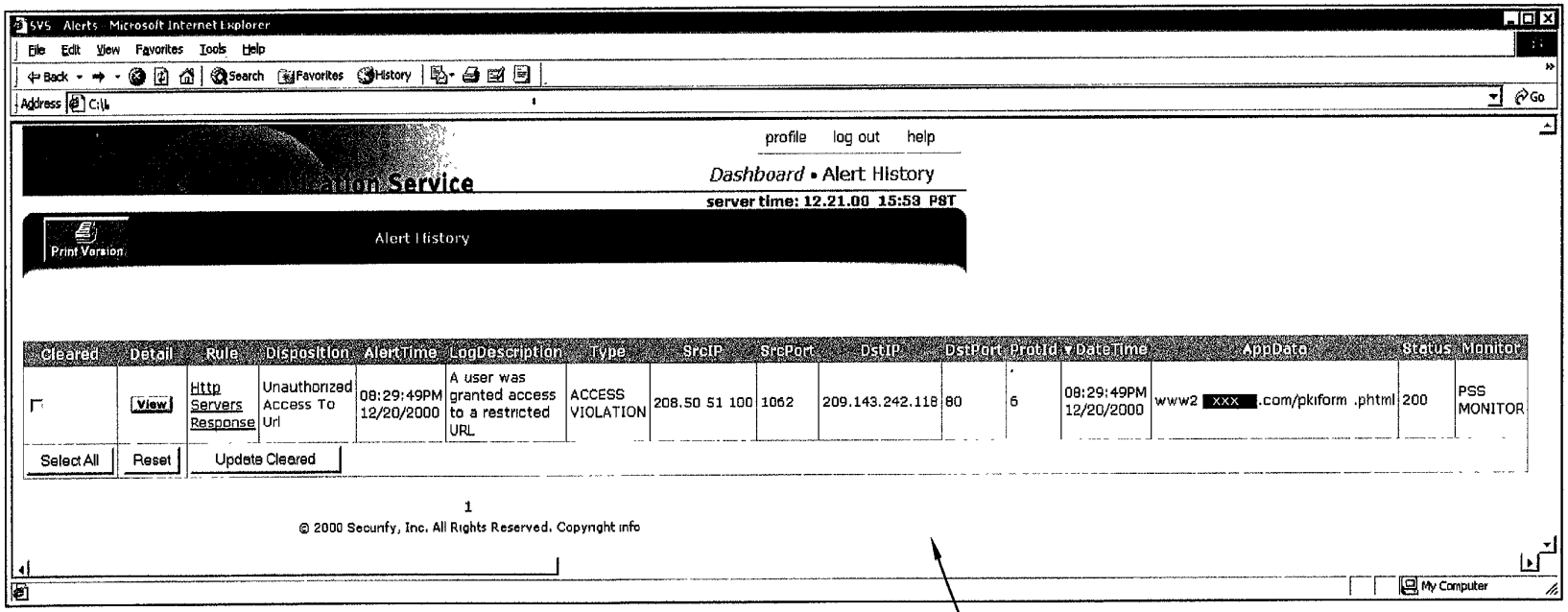

SVS Alerts Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\
profile log out help
tion Service
Dashboard • Alert History
server time: 12.21.00 15:53 PST
Print Version
Alert History
Cleared Detail Rule Disposition AlertTime LogDescription Type SrcIP SrcPort DstIP DstPort ProtId DateTime AppData Status Monitor
View
Http Servers Response
Unauthorized Access To Url
08:29:49PM 12/20/2000
A user was granted access to a restricted URL
ACCESS VIOLATION
208.50 51 100
1062
209.143.242.118
80
6
08:29:49PM 12/20/2000
www2 XXX .com/pkiform .phtml
200
PSS MONITOR
Select All
Reset
Update Cleared
1
© 2000 Securify, Inc. All Rights Reserved. Copyright info
My Computer
2801

FIG. 28

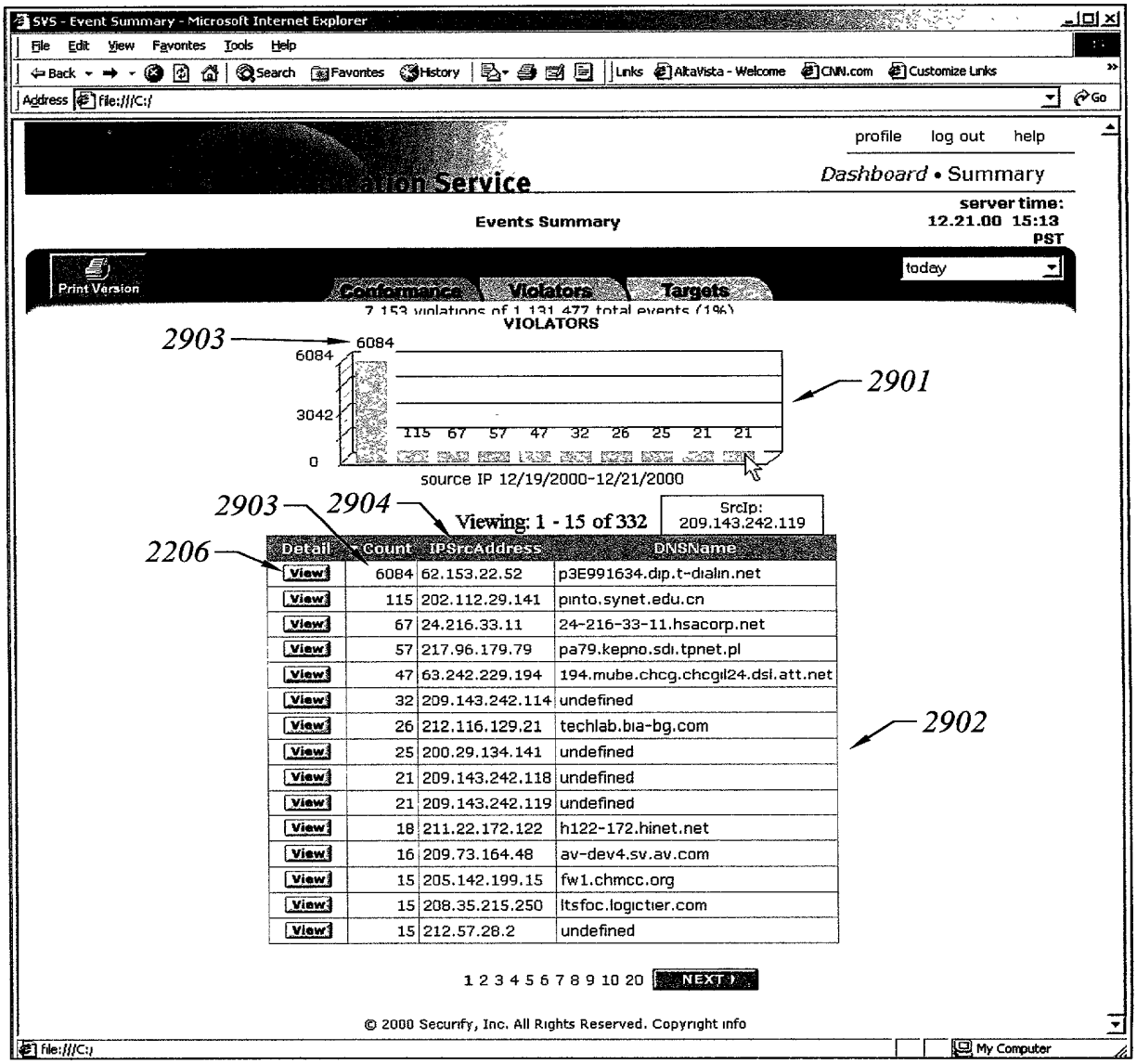

SV5 - Event Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links
Address file:///C:/
profile log out help
Dashboard • Summary
Events Summary
server time:
12.21.00 15:13
PST
Print Version
Conformance
Violators
Targets
today
VIOLATORS
2903
6084
3042
0
115 67 57 47 32 26 25 21 21
2901
source IP 12/19/2000-12/21/2000
2903
2904
Viewing: 1 - 15 of 332
SrcIp:
209.143.242.119
2206
Detail
Count
IPSrcAddress
DNSName
View 6084 62.153.22.52 p3E991634.dip.t-dialin.net
View 115 202.112.29.141 pinto.synet.edu.cn
View 67 24.216.33.11 24-216-33-11.hsacorp.net
View 57 217.96.179.79 pa79.kepno.sdi.tpnet.pl
View 47 63.242.229.194 194.mube.chcg.chcgil24.dsl.att.net
View 32 209.143.242.114 undefined
View 26 212.116.129.21 techlab.bia-bg.com
View 25 200.29.134.141 undefined
View 21 209.143.242.118 undefined
View 21 209.143.242.119 undefined
View 18 211.22.172.122 h122-172.hinet.net
View 16 209.73.164.48 av-dev4.sv.av.com
View 15 205.142.199.15 fw1.chmcc.org
View 15 208.35.215.250 ltsfoc.logictier.com
View 15 212.57.28.2 undefined
2902
1 2 3 4 5 6 7 8 9 10 20 NEXT
© 2000 Securify, Inc. All Rights Reserved. Copyright info
file:///C:/
My Computer

FIG. 29

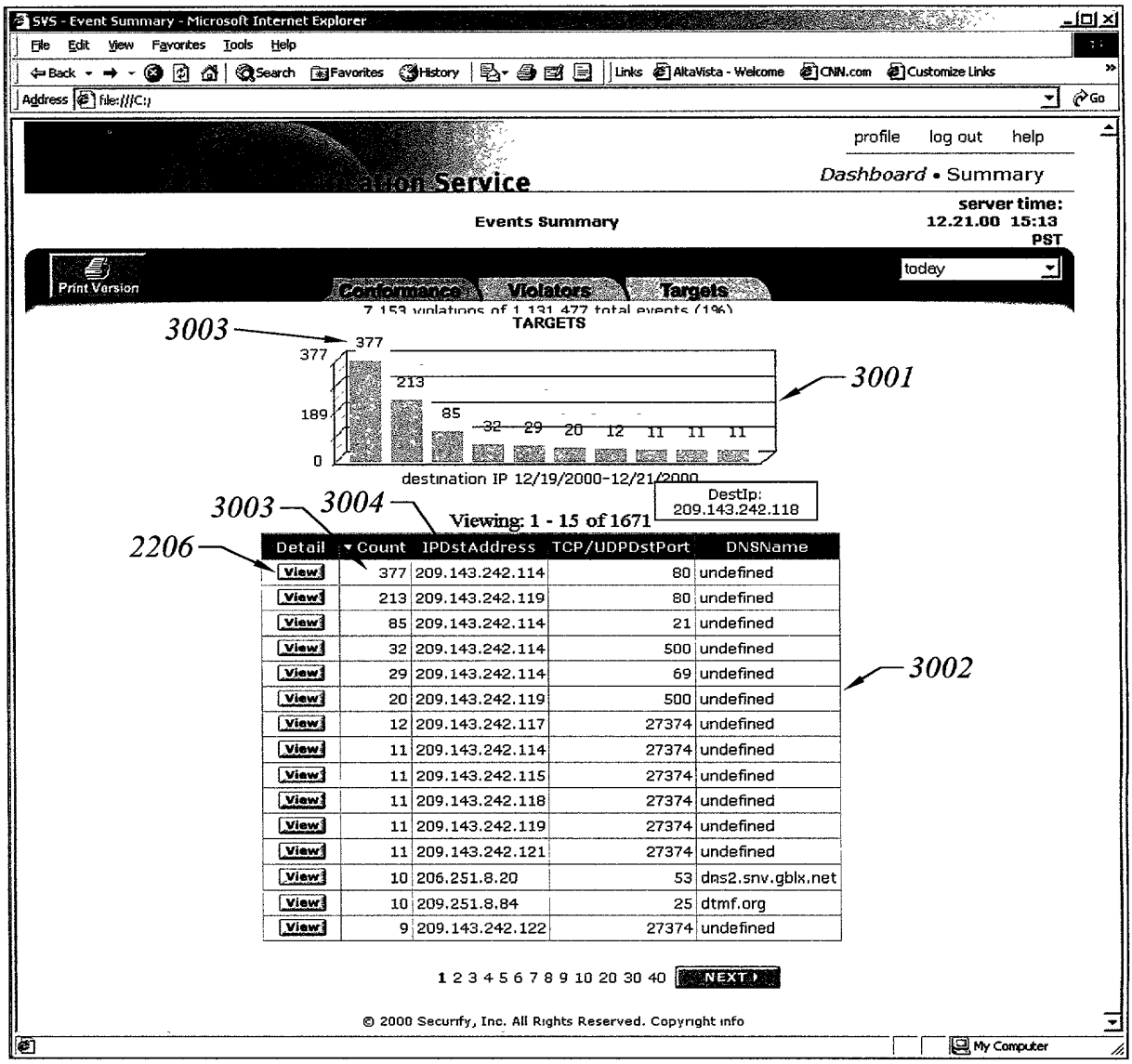

SVS - Event Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links
Address file:///C:/
profile log out help
Dashboard • Summary
Events Summary
server time:
12.21.00 15:13
PST
Print Version
Performance
Violators
Targets
today
7,153 violations of 1,131,477 total events (1%)
TARGETS
3003
3001
377
213
85
32
29
20
12
11
11
11
189
0
destination IP 12/19/2000-12/21/2000
DestIp:
209.143.242.118
3003
3004
Viewing: 1 - 15 of 1671
2206
3002
Detail
Count
IPDstAddress
TCP/UDPDstPort
DNSName
View 377 209.143.242.114 80 undefined
View 213 209.143.242.119 80 undefined
View 85 209.143.242.114 21 undefined
View 32 209.143.242.114 500 undefined
View 29 209.143.242.114 69 undefined
View 20 209.143.242.119 500 undefined
View 12 209.143.242.117 27374 undefined
View 11 209.143.242.114 27374 undefined
View 11 209.143.242.115 27374 undefined
View 11 209.143.242.118 27374 undefined
View 11 209.143.242.119 27374 undefined
View 11 209.143.242.121 27374 undefined
View 10 206.251.8.20 53 dns2.snv.gblx.net
View 10 209.251.8.84 25 dtmf.org
View 9 209.143.242.122 27374 undefined
1 2 3 4 5 6 7 8 9 10 20 30 40 NEXT
© 2000 Securify, Inc. All Rights Reserved. Copyright info
My Computer

FIG. 30

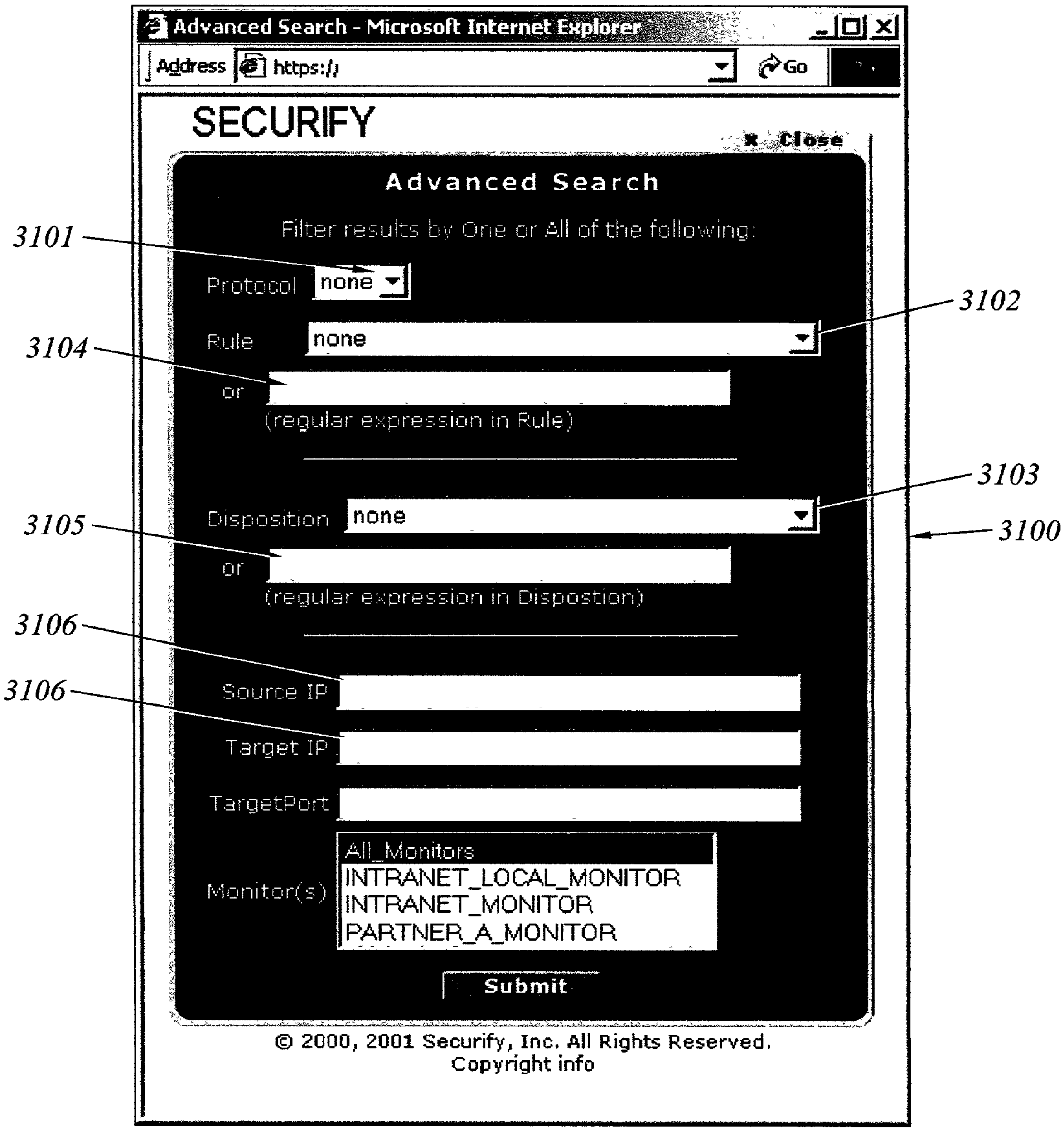
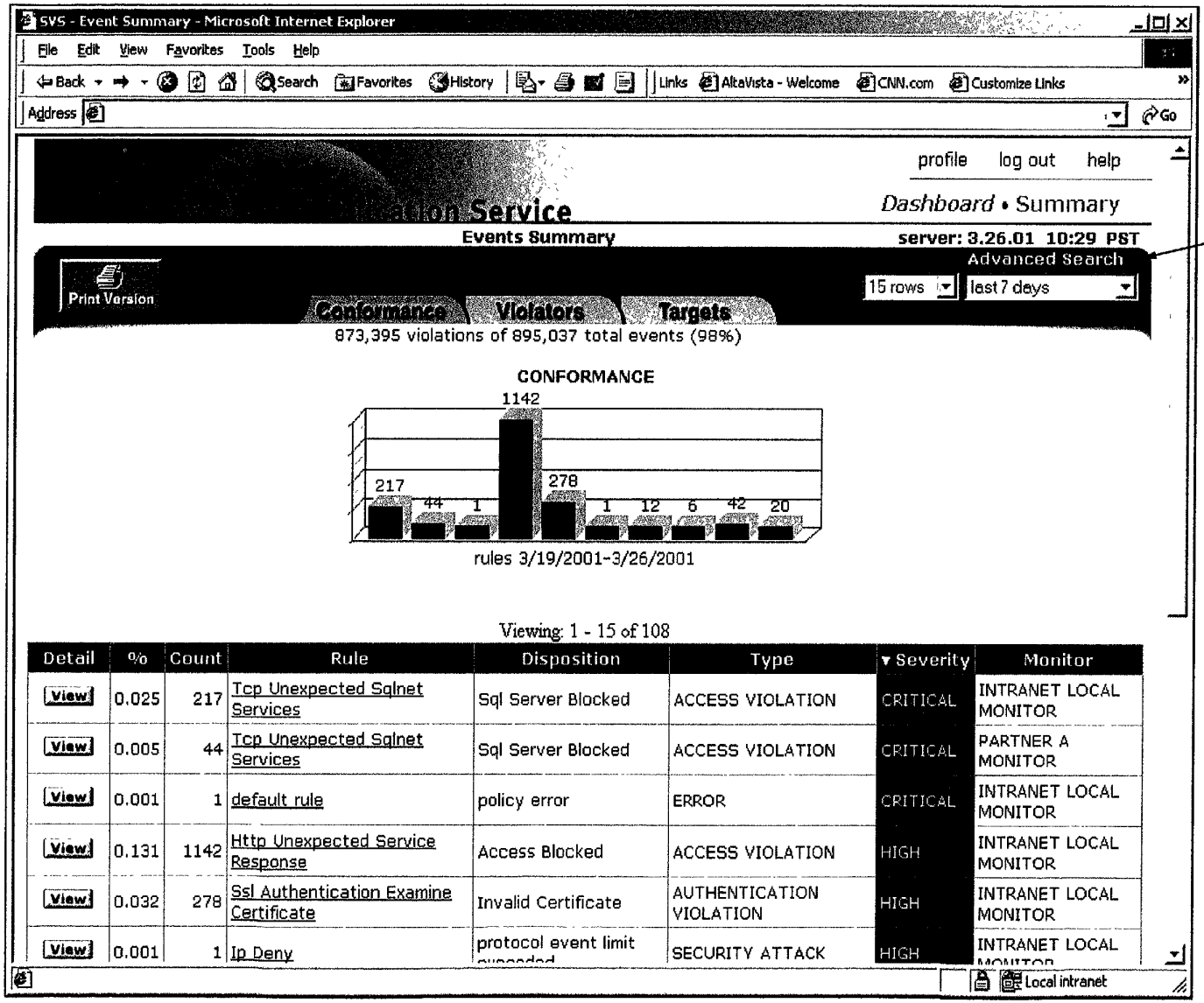

Advanced Search - Microsoft Internet Explorer
Address
https://
Go
SECURIFY
Close
Advanced Search
Filter results by One or All of the following:
Protocol
none
Rule
none
or
(regular expression in Rule)
Disposition
none
or
(regular expression in Dispostion)
Source IP
Target IP
TargetPort
Monitor(s)
All_Monitors
INTRANET_LOCAL_MONITOR
INTRANET_MONITOR
PARTNER_A_MONITOR
Submit
© 2000, 2001 Securify, Inc. All Rights Reserved.
Copyright info
3101
3102
3103
3104
3105
3106
3106
3100

FIG. 31


SVS - Event Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links
Address
Go
profile log out help
Dashboard • Summary
Events Summary
server: 3.26.01 10:29 PST
Advanced Search
Print Version
15 rows
last 7 days
Conformance
Violators
Targets
873,395 violations of 895,037 total events (98%)
CONFORMANCE
1142
217
44
1
278
1
12
6
42
20
rules 3/19/2001-3/26/2001
Viewing: 1 - 15 of 108
Detail | % | Count | Rule | Disposition | Type | ▾ Severity | Monitor
View | 0.025 | 217 | Tcp Unexpected Sqlnet Services | Sql Server Blocked | ACCESS VIOLATION | CRITICAL | INTRANET LOCAL MONITOR
View | 0.005 | 44 | Tcp Unexpected Sqlnet Services | Sql Server Blocked | ACCESS VIOLATION | CRITICAL | PARTNER A MONITOR
View | 0.001 | 1 | default rule | policy error | ERROR | CRITICAL | INTRANET LOCAL MONITOR
View | 0.131 | 1142 | Http Unexpected Service Response | Access Blocked | ACCESS VIOLATION | HIGH | INTRANET LOCAL MONITOR
View | 0.032 | 278 | Ssl Authentication Examine Certificate | Invalid Certificate | AUTHENTICATION VIOLATION | HIGH | INTRANET LOCAL MONITOR
View | 0.001 | 1 | Ip Deny | protocol event limit | SECURITY ATTACK | HIGH | INTRANET LOCAL
Local intranet

3201

FIG. 32